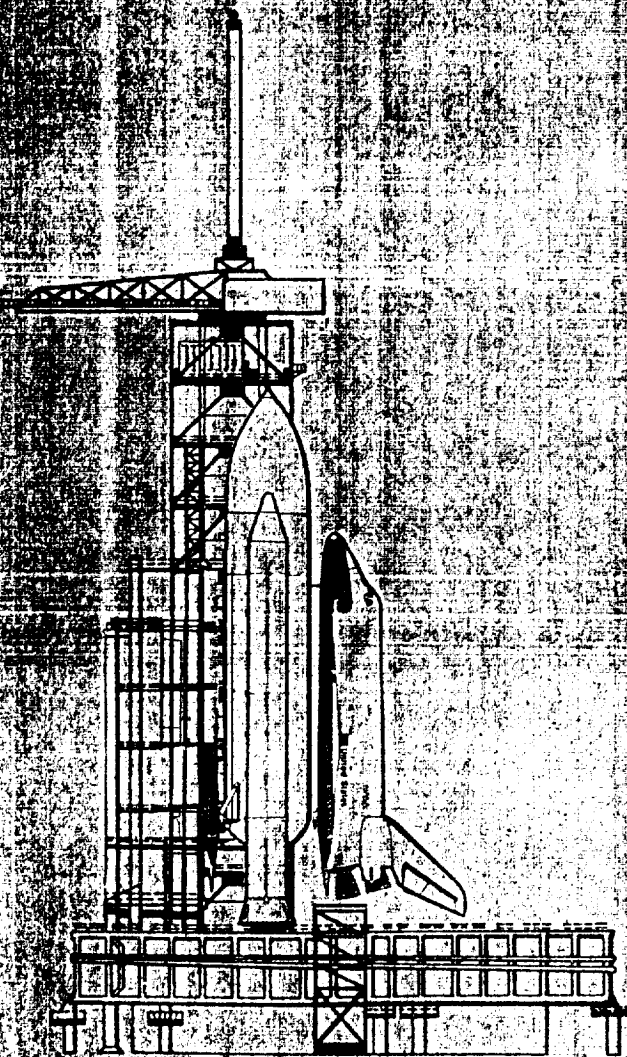


7N 76

Final Report of the STS Safety Risk Assessment Ad Hoc Committee

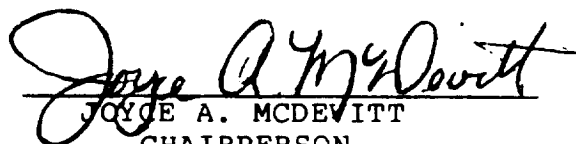
August 1987



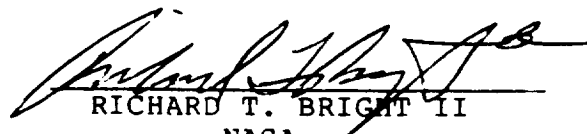
NASA

Office of the
Associate Administrator
for Safety, Reliability,
Maintainability and
Quality Assurance

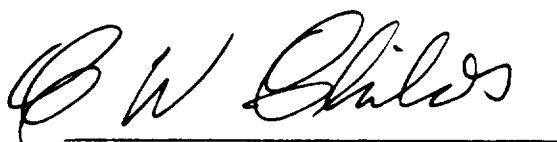
AT THE REQUEST OF THE NASA ASSOCIATE ADMINISTRATOR FOR
SAFETY, RELIABILITY, MAINTAINABILITY AND QUALITY ASSURANCE,
THE UNDERSIGNED PRESENT THE REPORT ON
THE REVIEW OF THE STS SAFETY RISK MANAGEMENT SYSTEM



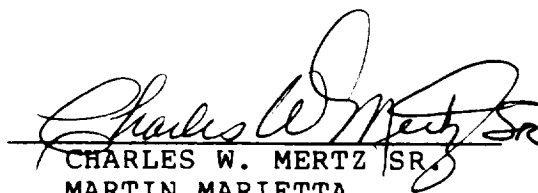
JOYCE A. MCDEVITT
CHAIRPERSON
NASA HEADQUARTERS



RICHARD T. BRIGHT II
NASA
LANGLEY RESEARCH CENTER



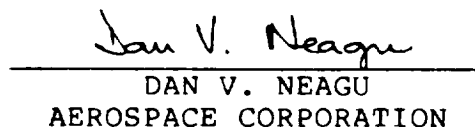
CHARLES W. CHILDS
RISK MANAGEMENT ASSOCIATES



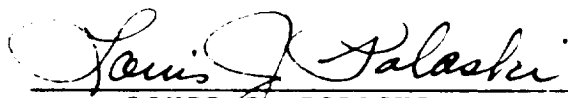
CHARLES W. MERTZ SR.
MARTIN MARIETTA



LTC JONATHAN B. MULLIN
U.S. AIR FORCE
WESTERN SPACE AND MISSILE CENTER



DAN V. NEAGU
AEROSPACE CORPORATION



LOUIS J. POLASKI
NASA
AMES RESEARCH CENTER



JAMES H. WIGGINS
TECHNICAL ANALYSIS INC

TABLE OF CONTENTS

	PAGE
I. Executive Summary.....	1
II. The Committee Charter, Organization, and Review Process.....	4
III. Summary of Major Observations.....	7
IV. Vacillating Safety Emphasis.....	12
V. The NASA Safety Organization and Management.....	17
VI. Policy and Requirements.....	33
VII. Skilled Safety Personnel.....	38
VIII. Personnel Motivation.....	40
IX. Safety Assessment Review Process.....	44
X. Reassessment of STS Hazard Analyses.....	47
XI. Launch Decision Waiver Process.....	51
XII. Safety Requirements in the NSTS Contracts.....	53
XIII. Safety Assessment Information Systems.....	57
XIV. List of Recommendations and Action Responsibilities....	60
Appendix A. Charter of the Committee	
Appendix B. The NASA/NSTS Safety Organization	
Appendix C. The Space Station Safety Organization	
Appendix D. The Code Q System Safety Organization	
Appendix E. NSTS Policy and Requirements	

I. EXECUTIVE SUMMARY

On November 6, 1986, The NASA Associate Administrator for Safety, Reliability, Maintainability, and Quality Assurance (AA/SRM&QA) appointed the STS Safety Risk Assessment Ad Hoc Committee to conduct an independent review of the safety risk management system for the National Space Transportation System (NSTS) program. To bring objectivity to the review, the Committee members were selected from NASA Headquarters, two NASA Aeronautical Research Centers, Department of Defense, large aerospace corporations, and safety support services organizations.

The review addressed the NSTS safety requirements, process, documentation and the safety organizations' involvement in all levels of the NSTS decision-making process. Detailed presentations were provided by the NSTS Program Levels I, II, and III organizations, NSTS Level IV element contractors, and several NASA and contractor payload organizations during the period from November 17, 1986 to February 6, 1987. The Committee's report is based upon observations and statements of facts and opinions from NASA managers and personnel and NASA contractor managers and personnel with extensive experience in space program engineering management, operations, safety, reliability, and quality assurance. In gathering this information, the Committee talked to many of the key people in the NSTS program and attempted to reach the most knowledgeable sources; however, in a few cases, key people were not available. In response to the Committee's request and stated intent to treat the information as generically as possible, many of the organizations provided an input on perceived inhibitors and barriers to effective safety management. In turn, recommendations were made which should improve the present NASA and NSTS safety management.

The Committee's observations and recommendations address problems associated with the vacillating NASA management emphasis on safety, the NASA and NSTS safety organization and management, safety policy and requirements, skills of safety personnel, personal motivation, the safety assessment review process, the reassessment of NSTS hazard analyses, the launch decision waiver process, safety requirements in the NSTS contracts, and the safety assessment information systems. Seventy-two recommendations are suggested to correct these problems, and the organizations which are responsible for their implementation have been identified.

The recommendations considered by the Committee to have the highest priority for the next NSTS flight address the need for revitalizing a vigorous and extensive Manned

Space Flight Motivation Program and providing for an immediate infusion of space system engineering skills into the NASA and support contractors' safety organizations. It is essential that NASA management provide the necessary leadership in addressing these issues. It is important that the entire NASA and contractor workforce be convinced that safety is important to management and that it is a necessity for every individual to make a personal commitment to excellence in order to assure NSTS mission success.

Several recommendations which are essential to providing an "arm's length" independent safety assessment system supported by safety information data bases and trend analyses are also critical. These recommendations address a strengthening of the NSTS safety management integration function to enhance the NSTS aggregate safety risk assessment and a restructuring of the NSTS and NASA assurance organizations to provide the independent safety assessment. Considerable planning and detailed work, including interim solutions for the next launch decision, are required to provide a thorough and independent safety assessment - a new concept for NASA.

The STS Safety Risk Assessment Ad Hoc Committee tried to surface safety management areas in need of improvement and issues that are important to address in order to provide a strong independent safety review for NSTS. In emphasizing those things which are wrong, there is always a risk of conveying an impression that nothing is right. Obviously, this is not the case. The Committee recognizes that if NASA had not done so many things right in the past, our Nation's space capability would still be struggling to accomplish its first significant achievements. On the other hand, the Challenger accident did emphasize to us all that there were some vital improvements needed to approach the degree of acceptability required for low risk manned space flight.

It should be recognized also that the review was conducted over a period of time when there were significant NASA efforts underway to identify and correct some of the same deficiencies cited in this report. As a result, there are some on-going actions which will undoubtedly serve the process of implementing the recommendations.

The Committee acknowledges that there is little recognition given in the report to those organizations which had effective safety programs in place and the many positive actions being taken to effect still greater improvement in safety management throughout the agency. The tremendous support of literally hundreds of people in preparation for this Committee's review is testimony to

their outstanding dedication. The Committee wishes to thank these people for their cooperation and patience.

Finally, the Committee hopes that this report will be received in the light of constructive criticism and that implementation of the recommendations will result in a stronger NSTS program which we all believe is essential to out National well-being.

II. THE COMMITTEE CHARTER, ORGANIZATION, AND REVIEW PROCESS

The Committee Charter and Organization

The NASA Associate Administrator for Safety, Reliability, Maintainability, and Quality Assurance on November 6, 1986, appointed an ad hoc committee to conduct an independent review of the safety risk management system for the National Space Transportation System program. The memorandum which established the Committee and its charter is in Appendix A.

The Committee members were selected from NASA Headquarters, two NASA Aeronautical Research Centers, Department of Defense, large aerospace corporations, and safety support services organizations. The members were selected for their objectivity and extensive experience in system safety, reliability, quality assurance, project management, organizational management, budgeting and contracting. The Committee members and their respective organizations were as follows:

Joyce A. McDevitt	Chairperson, NASA Headquarters
Richard T. Bright, II	NASA-Langley Research Center
Charles W. Childs	Consultant, Risk Management Associates, Inc.
Charles W. Mertz, Sr.	Consultant, Martin Marietta Orlando Aerospace
Jonathan B. Mullin	LTC, USAF, Western Space and Missile Center
Dan V. Neagu	Consultant, Aerospace Corporation
Louis J. Polaski	NASA-Ames Research Center
James H. Wiggins	Consultant, Technical Analysis, Inc.

Frederic Sponholz, NASA-Johnson Space Center Safety Division, was an observer to the Committee.

The Committee was chartered to conduct an independent and systematic assessment of the NSTS safety requirements, process, documentation and the safety organizations' involvement in all levels of the NSTS decision process. Also, the Committee was to determine what the integrity of the NASA and NASA contractor safety risk management program was at the time of the Challenger mishap, what it

was at the time of the Committee review, and what it is planned to be in support of the next launch.

An Overview of the Committee Review Process

The Committee utilized a "bottoms-up" approach in performing the safety review of the NSTS program, that is, the NSTS Level IV element contractors were visited first. The Level IV organizations included Rockwell International (Orbiter and Integration), Rocketdyne (Space Shuttle Main Engine), Morton Thiokol, Inc. (Solid Rocket Motor), USBI (Solid Rocket Booster), Martin Marietta (External Tank), and Lockheed (Shuttle Processing). Visits were then made to Level III organizations (Kennedy Space Center, Marshall Space Flight Center, and Johnson Space Center), Level II (Johnson Space Center), and Level I (NASA Headquarters). In addition, the STS payload safety review process was addressed at TRW, Hughes, McDonnell Douglas, Teledyne Brown, Goddard Space Flight Center, Jet Propulsion Laboratory, Johnson Space Center, and Marshall Space Flight Center. Safety services contractors included EBON and EG&G at Kennedy Space Center and Boeing Aerospace Operations at Johnson Space Center. Also, the Air Force provided a summary review of their approach to tailoring the NASA requirements to facilities and launch processing activities; however, the thrust of this review was directed to the NASA safety program and safety resources in support of the NSTS program.

The reviews were conducted during the period from November 17, 1986 to February 6, 1987. The review consisted of detailed presentations by each organization to address the Committee-designated topical areas with further questioning by the Committee following the presentations. Because the time spent with each organization was limited, a list of detailed questions was provided to clarify the agenda, and a documentation package was requested from each organization in advance.

The "bottoms-up" approach provided the Committee with an insight into how a safety risk would be managed within an organization, reviewed, and, in the end, accepted as it was passed up the management chain from Level IV to Levels III, II, and I for resolution. The more significant safety issues that were addressed by the Committee and served as a common thread in the data gathering phase of the review included those associated with the SRB field joints and seals, the problem of the SSME turbine blades, the "handing off" of hardware and hazards analysis results, adherence to upper level requirements, the management risk acceptance process, and manager's risk acceptance criteria.

A concerted effort was made by the Committee to obtain the center and program/project management perspective in addition to that of the safety organization. The management perspective was most beneficial in developing an understanding of the entire safety review process including that which is embedded in engineering and operations and how the contributions and outputs from the safety organizations support the management decisions and provide for an independent safety assessment.

The Committee's stated intent to treat the information as generically as possible provided each organization an opportunity to discuss perceived inhibitors and barriers to effective safety management and provide recommendations which would enhance the NSTS Safety Program. This input was evaluated by the Committee in developing its final observations and recommendations.

The Committee developed the major issues addressed in this report in a working meeting after all the visits to the organizations were completed. Subsequently, all observations and recommendations were developed in Committee working meetings, and these observations and recommendations are reflected in this report. Additional Committee reviews of draft iterations of the report resulted in a total consensus and signature approval by all of the Committee members.

III. SUMMARY OF MAJOR OBSERVATIONS

These observations and recommendations are considered by the Committee to have the highest priority for implementation in order to enhance the NSTS Safety Risk Management Program and assure the readiness of the Program in support of the next NSTS flight. These priority concerns are those that deal primarily with the **people**, the **management**, and the **independent safety assessment** in that order.

THE PEOPLE

Personnel Motivation: Much of the inspiration for excellence in workmanship, personal dedication and the notion that we should look beyond our individual jobs in making sure that risks for space travel are minimized has been lost over the years between the successful Apollo missions and the Challenger accident. It is not too difficult to understand this in light of the perceived routine nature of space flight. It took the rude shock of the Challenger disaster to bring us to the reality that manned space flight is not routine. It takes the same attention to detail and the same personal integrity and dedication to excellence in workmanship as there was during the days when the initial space quests inspired all of us. Recommendations: NASA management must provide the leadership and the inspiration to rekindle a team spirit and pride of accomplishment. The importance of personal dedication must be made clear to every individual in the manned space program. A vigorous and extensive manned space flight motivation program must be revitalized. The importance of manned space flight to national prestige, to the progress of science and technology, and to the aspirations of mankind must be emphasized.

Skilled Safety People: There is a critical lack of space systems engineering skills within NASA and NASA support contractors' organizations. In order to provide meaningful hazard analyses and safety assessments, safety engineers need to be competent not only in the system safety discipline but also in the areas of design, fabricating processes, test, and operational aspects of the hardware and software systems which must be evaluated for safety risks. In addition, these engineers must be motivated to define all the details of a safety concern and must press aggressively for hazard controls. If they do not possess these skills, the hazard analyses, which are the cornerstones of the risk assessment, are usually incomplete and superficial. It is unlikely that this situation will improve or that a meaningful safety assessment can be made without a change in management policy and a redirection of personnel resources. In the

end, there must be recognition and rewards not only for the primary doer but also for those whose job it is to question, probe, and independently assess risks.

Recommendations: NASA management must provide for an immediate infusion of systems engineers into the safety organizations and develop a structured system safety career path which can offer satisfaction, personal recognition, training, and promotion opportunities. Contractors should be encouraged to do so as well.

THE MANAGEMENT

Vacillating Safety Emphasis: Since the advent of manned space flight, there has been an alarming vacillation in management's safety emphasis. The 1967 Apollo accident and the Apollo 13 incident peaked the concern for safety, and the mission successes in between and after took the edge off some of the natural cautions for safety. This problem is one dealing primarily with human nature because people do not like to be reminded of the unpleasantness and pain associated with accidents. In addition, as tasks become more and more routine, workers are apt to forget the cautions and safeguards that were developed through bitter accident experience. This is further complicated by the fact that a successful safety program which minimizes accidents may be indirectly responsible for this waning concern. NASA top management commitment to safety is evidenced by the appointment of an Associate Administrator for Safety, Reliability, Maintainability, and Quality Assurance. It remains to be seen if this will result in a strong system safety effort and a continuing resolve to maintain a strong commitment to safety.

Recommendations: NASA management must provide adequate resources for safety management immediately and maintain a consistent level of effort through periods of success as well as periods of adversity.

Management Emphasis Today: After the Challenger accident, the concern for space flight safety was overwhelming both in NASA and the outside world. It was inevitable that some of this concern would fade with the passage of time. However, there are disturbing signs that some of the pre-51L safety related problems which were identified in the aftermath of the accident still exist. Some typical examples are: (1) in the review of a safety critical redesign, the hazard analyses are being done after the fact, not as a critical assessment used to support the design decision; (2) one of the principal NSTS contractors whose safety efforts for reassessment were lagging made no significant effort to fill authorized safety engineering vacancies with qualified safety professionals; (3) there is a general lack of concern for checking interface controls and integration hazards; and

(4) there is still evidence of errors in assembly and processing and improper quality and supervision sign-offs on flight critical items. The concern for NSTS safety which peaked shortly after the Challenger accident appears to be waning, and in many areas this has been translated by workers, engineers and supervisors to a "business as usual" attitude. **Recommendations:** NASA management at all levels must make a personal commitment to openly and actively support safety by all of their actions so that the safety concern is translated into everyday direction and each person understands the necessity for disclosure of safety problems to assure NSTS mission success. NASA management should begin by expressing the commitment to safety as a part of a National Space Policy and a NASA top level management policy for manned space flight.

NSTS Safety Management and Integration: The NSTS safety management integration effort is not adequately defined and does not provide for complete independence of a Level II review in the overall NSTS safety program review process. This situation was caused, in part, by a conscious reduction of the NSTS management oversight and contractor integration management effort with the announcement that the NSTS was operational. In addition, there was a "hybrid" system safety/engineering function which evolved after the Apollo accident. This caused confusion because in-line program engineering continued to have the responsibility for addressing safety considerations in the design and operations tradeoffs. In-line engineering also developed the safety requirements and the criteria for safety margins verification and validation. The system safety function which should establish the basic safety requirements and assure requirements are met was used, in many cases, to document and sanction the program engineering process. Also, it remains to be seen if the hazard analysis revalidation activities and documentation will assure that a complete integrated end-to-end assessment has been made. If an end-to-end assessment is not done in a thorough and coordinated manner, any aggregate safety risk assessment is going to be made with suspect incremental risk information. **Recommendations:** The position of SR&QA at Level II should be elevated to a NSTS Program Deputy Director level and the safety integration management refined to include primary responsibilities for each part of the NSTS system from design through manufacture to complete assembly, operation, launch, landing, and maintenance.

THE INDEPENDENT SAFETY ASSESSMENT

The NASA/NSTS Safety Organization: NASA program and safety managers interviewed had different interpretations of the degree of independence that was necessary to provide the required independent safety assessment for each NSTS flight. For most part, they were looking for some detailed guidance and direction from the NASA Headquarters Office of SRM&QA.

The Committee, in pondering how this independent assessment could be done, arrived at several important conclusions. First, the primary responsibility for NSTS safety must remain, as it always has, with the program manager. Second, there must be a concerted effort to keep the independent safety assessment as separate as possible from the program safety management in order to avoid any perceived conflict of interest. Third, a completely independent assessment is not feasible. It was recognized that absolute independence would require almost as many technically qualified people on the assessment team as there are in the entire program.

In addressing an acceptable rather than absolute independence, it became apparent that the assurance management must be careful to retain an "arm's length" relationship in order to maintain an acceptable degree of objectivity. It was also apparent that there would be times when the assurance community would have to work for the program, and at other times side-by-side with the program, in order to understand and solve safety problems. This intertwining of work tasks and responsibilities could make an independent safety assessment difficult, and also it could exacerbate all of the conflict of interest negatives involved in a matrix organization. Despite this, the Committee felt that if it is done carefully, there is promise for an acceptable independent safety assessment process.

However, there are some present difficulties in achieving this acceptable independent safety assessment system.. First, the current roles, responsibilities, and activities within Code Q force this organization to be a part of the program management in-line function and decision process at Level II. In turn this can make a Level I independent safety assessment a difficult, if not impossible, job. Second, some of the NSTS safety community has not accepted the premise that the program manager is, and should be, primarily responsible for the safety of the NSTS program. If this attitude prevails, it could result in the independent safety assessment being a "rubber stamp" of the NSTS in-line safety decision process. It could also preclude the program manager from combining the

proper measures of safety, technical performance, cost and schedule controls to assure mission success.

To rectify this entire situation and to respond to the current executive and congressional directions, there must be some changes made in both the program and assurance organizations and in the mind-set of key management people. There must also be a meticulous definition of roles and responsibilities which will be needed to keep the two management systems functioning efficiently and objectively. **Recommendations:** NASA management should revise both program and assurance organizations and define responsibilities to foster an independent safety assessment and move quickly to fill the key positions so that the independent safety assessment for the next launch is thorough and timely. A plan for implementation of the independent safety assessment should be developed to address both the short term and long term objectives, activities, and inputs necessary to make the launch decision.

IV. VACILLATING SAFETY EMPHASIS

History has proven that, in the area of safety, management attention and emphasis follows cycles of highs and lows. The Committee is concerned about the negative impact of this vacillating safety emphasis to the NASA Manned Space Flight Program.

A. HISTORICAL PERSPECTIVE

1. OBSERVATION:

Since the advent of manned space flight, there has been an alarming vacillation in safety emphasis and management.

2. DISCUSSION:

The difficulty in maintaining a proper level of concern for safety over long periods is primarily a problem of human nature. People do not like to be reminded of the unpleasantness and pain associated with accidents. In addition, as tasks become more and more routine, workers are apt to forget the cautions and safeguards that were developed through bitter accident experience. This is further complicated by the fact that a successful safety program which minimizes accidents may be indirectly responsible for this waning concern. After all, "who wants to pay for a program that is obviously not needed. Nothing bad is happening." As obvious as the fallacy of this thinking is, in retrospect, it is difficult to prove before an accident that all of the actions taken in the name of the safety program would actually have prevented the accident.

Over a period of years starting with the first manned program, NASA has been plagued with this vacillating concern for safety. The 1967 Apollo accident and the Apollo 13 incident peaked the safety concern, and the mission successes, in between and after, took the edge off some of the natural cautions for safety. Added to this, NASA has had a propensity over the years to relegate the Headquarters Safety function to various different organizations as a consequence of management's lack of concern or as a move to solve organizational or personnel problems. As a result, there were many confusing moves and mergers, changes in directors and direction, and in one instance a proposal to eliminate entirely all of the assurance disciplines at Headquarters. In addition, basic requirements for system safety

in contracts were periodically changed by various administrative managers under the guise of economy and, finally, were deleted from the procurement regulations three years ago. These actions contributed to frequent changes in direction and made it extremely difficult to deal with the waning safety interest syndrome.

There was still another consequence to the many changes in Headquarters management. The centers were encouraged to "mirror image" the Headquarters safety organizations. While this was in some cases impossible, the reorganizations in Headquarters always had some ripple effects on the center organizations. This resulted in further confusion in the roles and mission of these safety organizations and undoubtedly had some effects on the quality and efficiency of their efforts.

NASA top management's apparent commitment to safety is evidenced by the appointment of an Associate Administrator for Safety, Reliability, Maintainability, and Quality Assurance. It remains to be seen if this will result in a strong system safety effort. Further, a personal commitment is needed from NASA management at all levels to translate the safety concern into everyday direction. As one worker put it, "Their words say safety, but their actions say, don't worry about it."

There must be a continuing resolve to maintain a strong commitment to safety. History reveals to us that this will not be an easy job. We must constantly remind ourselves that space exploration is a risky venture and it will become more complicated and riskier as our quests become bolder. Finally, we must not be lulled into complacency by success. As one of our former NASA safety directors stated during the Apollo time period, "Complacency feeds on success."

3. RECOMMENDATIONS:

- a. Immediately provide adequate resources for safety management and maintain a consistent level of effort through periods of success as well as periods of adversity.
 - (1) Obtain a firm management commitment required to implement the Conceptual Plan for a NASA Headquarters Enhanced Safety Program.

- (2) Update and distribute an approved implementation plan annually to include long range projected needs.
- (3) Evaluate center level implementation plans and apprise NASA top management of major differences between the needs of the organization and actual resources.

B. MANAGEMENT EMPHASIS ON SAFETY TODAY

1. OBSERVATION:

The concern for NSTS safety which peaked shortly after the Challenger accident appears to be waning and in many areas this has been translated to a "business as usual" attitude.

2. DISCUSSION:

After the Challenger accident the concern for space flight safety was overwhelming both in NASA and in the outside world. It was inevitable that some of this concern would fade with the passage of time. There was a need to get on with the job - a job which entails some significant risks.

The Committee looked for some indications of how far this concern for safety had waned. It was concluded that there were disturbing signs that some of the pre-51L safety-related problems which were identified in the aftermath of the accident were still there.

There was evidence that some managers believed that procedures were followed as written. There was very little evidence that reasonable checks were made to assure that this was done. There is still evidence of errors in assembly and processing and improper quality and supervision sign-offs on flight critical items.

There have been a series of handling incidents and a recent serious handling accident with a flight critical component with implications of improper rigging, lack of training and improper supervision.

There is a general lack of concern for checking interface controls and integration hazards. Such comments as "It is not my responsibility. I have my own problems," were voiced by managers with hardware "hand-over" responsibilities.

There are some NASA technical monitors for major contractors who are evaluating safety engineering reassessment efforts by percentage completion summary information rather than reviewing specific analyses.

A NASA Center Project Managers' Handbook states that the project managers will be judged for effectiveness on cost, schedules and some reliability factors. Conspicuous by its absence was any mention of safety as a performance evaluation factor for these NASA project managers.

In the review of a safety critical redesign, the hazard analyses are being done to reflect the design selection. This follows the pre-51L pattern of safety documentation of risk decisions rather than a proactive safety analysis which influences the design.

Hazards are closed when a control is identified. There was little evidence that controls are verified as a routine management requirement.

One of the principal NSTS contractors whose safety efforts for reassessment were lagging made no significant effort to fill authorized safety engineering vacancies with qualified safety professionals.

There was a series of individual "aside" comments made by workers and managers that the priorities had shifted back to schedule first. As one worker put it, "We are now back to business as usual. The schedule comes first."

Although there are always some safety critical comments that can be attributed to unwarranted concerns and "hand wringing", the frequency of complaints heard by the Committee is in itself an unhealthy condition. It has long been recognized that safety is as much a condition of the mind as it is a technical discipline. The people who build and operate the Shuttle have to be convinced that safety is important to management. The concern must be translated into everyday direction. Modifications which are designed to decrease risks cannot be unduly delayed; waivers and deviations must be dispositioned formally with appropriate validation data; safety critical verification and validation tests should not be deleted to accommodate schedules and save costs; close-outs of safety problems and hazards must be tracked to assure that necessary actions are

actually being taken; and deviations to required procedures must be thoroughly and formally evaluated for safety impact.

The Committee found very little evidence that these concerns which are important to safety, and have not been done consistently in the past, were recognized as problems and would be given any priority to be properly done in the future.

3. RECOMMENDATION:

- a. Develop a National Space Policy and NASA top level requirements for manned space flight and make the commitment to safety a part of these policies. Such a commitment was clear in the words of President Kennedy, "I believe this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to earth."
- b. Demonstrate the commitment and resolve for safety in the development of a NASA top level management policy. (See Section VI)
- c. Assure that line managers down to first-line supervisors have a healthy concern for their role in providing safe flight.
- d. Make the commitment to safety a stated and integral part of each manager's career development.
- e. Evaluate the safety performance of each supervisor as part of their annual appraisal.

V. THE NASA SAFETY ORGANIZATION AND MANAGEMENT

The Committee selected certain major NSTS safety issues as "common threads" in their questioning to understand who was involved in the safety review process, how interface hazards were addressed, and the communications up and down the management chain in resolving and accepting safety risks. These discussions revealed inconsistencies in the approaches at each management level, apparent safety concerns being addressed as engineering or maintenance issues only, and some confusion whenever system or organizational interfaces were addressed. The Committee felt these problems were a result of both a weak Headquarters safety function and a weak NSTS safety integration process.

Background

The advent of manned space flight required a much higher level of systems integrity than obtained in previous missile programs. The concept of "manned rating" was used to describe the more extensive engineering analyses and testing done to verify and validate safety margins for both ground and flight systems. This process was conducted within the program engineering review procedures. During these early years the safety organizations had very little to do with this manned rating function. System safety was a relatively new discipline struggling to identify its mission and the tools of its profession.

The 1967 Apollo accident changed this. Suddenly it was realized that the program in-line engineering review process was not far reaching enough to provide all the safeguards and procedure reviews and not objective enough to voice all of the cautions needed for prudent decisions. A new safety organization was formed in the Office of Manned Space Flight, and system safety concepts were emphasized to provide additional safety assurance.

During this period, the analysis tools of this new discipline were still not as developed as those used in the program engineering function, and the safety engineers did not have the abilities nor the systems understanding to provide meaningful assessments. As a result, the application of system safety was limited. In many cases it was used to document and sanction the program engineering process. Fortunately during this period the rigorous program engineering review process was reemphasized, worst case scenarios were developed and reconciled, and seemingly everybody was involved in asking safety critical questions. Most importantly, the resources were provided to rectify the safety problems which were surfaced.

During the early Shuttle era, the system safety efforts expanded, but the deficiencies in the professional capabilities and understanding of the safety engineers precluded their playing a dominant role in the overall assessment process. The responsibility for addressing safety considerations in the design and operations tradeoffs and the development of requirements and criteria for safety margins verification and validation remained with, and still remains with, in-line program engineering.

A. ROLES AND RESPONSIBILITIES FOR THE NASA AND NSTS SYSTEM SAFETY PROGRAM

1. OBSERVATION:

The NASA and NSTS System Safety Program visibility, continuity and direction are not clear. Also the system safety function is fragmented and its application is inconsistent.

2. DISCUSSION:

The roles, responsibilities, and requirements of the NASA and NSTS System Safety Program are not clearly understood by program, safety, engineering, and operations managers. In addition, the principles of system safety are interpreted and being applied in the risk assessment process in almost as many ways as there are managers. This causes confusion and communications problems and can result in erroneous safety assessments. As an example, one contractor was holding open a residual hazard that had been closed three years before.

Another part of this confusion is the result of both a lack of definition of program integration management and misunderstandings between contractors and NASA organizations with primary responsibilities for the integration process. In turn this results in such deficiencies as having no effective hazard controls in transporting the SSME from the contractor's plant to the launch site. Presently the only controls for this transportation are the standard carriers' provisions in a general bill of lading.

On the positive side, there appears to be a general recognition that a well managed system safety effort can help identify and correct these integration inconsistencies. In turn, it appears to be recognized that this system safety effort must be a vital part of the engineering tasks

involved in design, processing of hardware and software, handling and shipping, vehicle buildup, margins verification and validation, and tracking of hazard controls in ground and flight operations. However, it remains to be seen if all of these essential functions will be properly emphasized. It also remains to be seen if the hazard analysis revalidation activities and requirements documentation will assure that a complete integrated end-to-end assessment has been made prior to the next launch.

Currently actions are being taken in reorganization and personnel assignments to correct some of these deficiencies and further integrate the system safety life cycle process into the NASA NSTS management program. However, some of these actions appear to be retrogressive. As an example in the reorganization that evolved after the establishment of the AA for SRM&QA, the system safety functions were parceled throughout the Code Q office. Yet, the primary job of establishing consistent NSTS policy, requirements and direction, evaluating the restructuring of center safety organizations, pulling all of these system safety functions together and evaluating the NSTS hazard reassessment effort primary falls on a one- person branch, which is the same unacceptable situation that existed prior to 51-L.

One inescapable conclusion that can be drawn from the integration and system safety management problems listed above is that, at present, any aggregate safety risk assessment made is likely to be flawed due to suspect incremental risk information.

3. RECOMMENDATION:

- a. Immediately take action to build a strong uniform system safety organization at Headquarters and throughout NASA.

B. THE STS SAFETY ORGANIZATION

Discussions were held with top SR&QA and NSTS management at the three NSTS centers and Headquarters to evaluate the capabilities of the NASA organization for providing an independent safety assessment for the NSTS program. Particular attention was given to the independence of the reviews at the various

organizational levels including the supporting safety review groups.

1. OBSERVATION:

All the managers interviewed had different interpretations about the degree of independence that was needed and could be provided to make the independent safety assessment for each STS flight.

2. DISCUSSION:

Several managers at one center indicated to the Committee that they hadn't come to grips with the independent safety assessment because they were going to be putting their best people "out there working on the program" and didn't have enough other qualified people to perform the independent safety function. At another center, the Center Director indicated that he felt responsible for maintaining the excellence of the products and services from the center and could personally provide that independent assessment through the launch readiness review decision if asked. Obviously, these statements are conflicting. The program is in a state of flux as to how the independent safety assessment will be made, who will be involved in the process, and what the specific roles and responsibilities of these individuals will be.

Some basic assumptions were made in looking at this problem of providing independent safety assessment. First, the program manager must retain the primary responsibility for the program safety. In turn, the program manager cannot be held responsible without having the authority to direct this function. Second, safety along with technical performance, cost control and schedules are essential program considerations which must be combined in proper measure to assure mission success. Third, there must be a mechanism to oversee the program safety function and assure that there is clear and continuing definition, measurement of, and disposition of safety risks in accordance with agency defined standards. Fourth, there must be a system to permit independent real-time review of all safety risk factors in assessing the prudence of program judgments leading to launch and mission operations.

Starting with these basic assumptions, the Committee concluded that making a thorough, completely independent safety assessment for NSTS

is not feasible because it would probably require as many technically qualified people in the assessment team as in the entire program. The NSTS system is too complex to be understood by a small group of people from the outside overlooking the process. The assurance disciplines must be a part of the engineering process to fully understand the problem. In some cases, the assurance organization must also participate in the solution of the problems. The real challenge is to maintain an acceptable degree of objectivity in the safety assessment process. On the other hand, program management must retain its primary responsibility for safety and assurance management and not give away its right to disagree and assess risks from program start through the launch decision process.

Stated another way, this dual safety contribution is sometimes referred to as the "doing" safety function and the "oversight" safety function. A separate "oversight" safety function is always needed because it is nearly impossible for someone to critically evaluate what they have done themselves.

In order to accomplish the dual roles, both program and assurance management must be careful to retain an "arm's length" relationship. In particular those individuals and organizations tasked to provide independent assessments cannot be the primary doers in making the everyday risk decisions. To assure that this is done, as a minimum, there should be one SR&QA manager at each level of management "hard lined" to the program. This manager should be responsible for managing the program risk decisions and assessments at his or her level for the Program Manager. Each program assurance manager could request matrixed help from assurance and engineering organizations on a full-time, part-time, or specific occasion basis to fill the continuing needs for the program risk control functions.

Those matrixed people who will be helping with the program doing functions, and on occasion will be called upon to "wear another hat" and furnish inputs to the independent safety function, must have special attributes beyond their technical capabilities. It is difficult to serve two masters. It also requires a very clear definition of the job to be done so that the matrixed person and each of managers involved understand their individual and collective roles from the start.

In the past the information, functions and responsibilities of programs and assurance management were so intertwined that it was nearly impossible to determine specifically what the risk issues were or look at the risk issues objectively. Assurance managers were making risk decisions for programs with limited information and with their assurance "hats" on. This made the independent safety assessment a difficult if not impossible job. One cannot be expected to do a job and then criticize oneself for not doing it correctly or completely.

Another situation that creates an apparent problem in the independence of the overall NSTS safety program review process is the continued identification of Level II with a center function. One center's SR&QA organization is serving in both a Level III and Level II capacity and reporting to the same manager. Also, this same situation exists for the safety services contractor supporting the center; personnel assigned to support Level III and II report to a single local manager in the same company. In addition, the chairpersons for the Shuttle System Safety Panel and the Senior Safety Review Board are identified primarily with the Level III function. Further, the reporting of the Chairperson of the NSTS Payload Flight Safety Review Panel to the payload integration organization presents a potential conflict in assuring both payload safety and also aiding payload developers in getting on the manifest of a particular mission. As currently structured, the NSTS program cannot be assured of a truly objective review at Level II in assessing and abating all risks resolved at Level III, particularly where controversial issues may be involved.

In addition to all of this, the relationship among the NASA Headquarters safety functions and the center safety organizations is not clearly defined. One example of the mixed signals coming from Headquarters is the recent issuance of an Office of Manned Space Flight (OMSF) organization which shows the OMSF Program Assurance Manager in a subordinate role which is significantly different from that approved for the Headquarters SRM&QA organization. Organization charts infer a relationship subject to the interpretation of each individual unless accompanied by clear, nonconflicting, functional statements of roles and responsibilities. The lack of written

accountability is seen as creating difficulties for program safety personnel who could receive conflicting advice and direction from several Headquarters offices, the NSTS management and center management.

To rectify this entire situation, there must be some changes made in both the program and the assurance organizations. In some cases, the solution is as simple as redefining responsibilities and moving people from one management system to another. In other cases it will require some reorganization, redefinition of the safety assessment review groups at each level and a reconstitution of the review groups to reflect both in-line and assurance managements' responsibilities. In any case it will require some change in the mind-set of key management people and a meticulous definition of roles and responsibilities in order to keep two management systems functioning efficiently and objectively. It will also be necessary to move quickly to fill those key positions so that the safety assessment for the next launch is thorough and timely.

A restructuring of the NASA/NSTS organization along the lines of Figure 1 is recommended. The proposed organization separates the program SR&QA function from the center's assurance functions and, most importantly, adds emphasis to the program Level II SR&QA function. The program and Center SR&QA relationship, shown for simplicity on the organization chart for only one center, is recommended for each Level III organization. To provide further definition to the proposed organization, the roles and responsibilities associated with the major safety elements are discussed in Appendix B. In addition, Appendix C presents a proposed organization for Space Station which parallels the proposed restructuring of the NASA/NSTS organization.

REASONS TO CREATE A SR&QA DEPUTY POSITION IN NSTS

The added NASA emphasis on the assurances which is manifest in the elevation of SRM&QA to Associate Administrator status should be reflected down through the program offices. This can be accomplished for the NSTS program by elevating the position of SR&QA at Level II to a Program Deputy Director.

NSTS

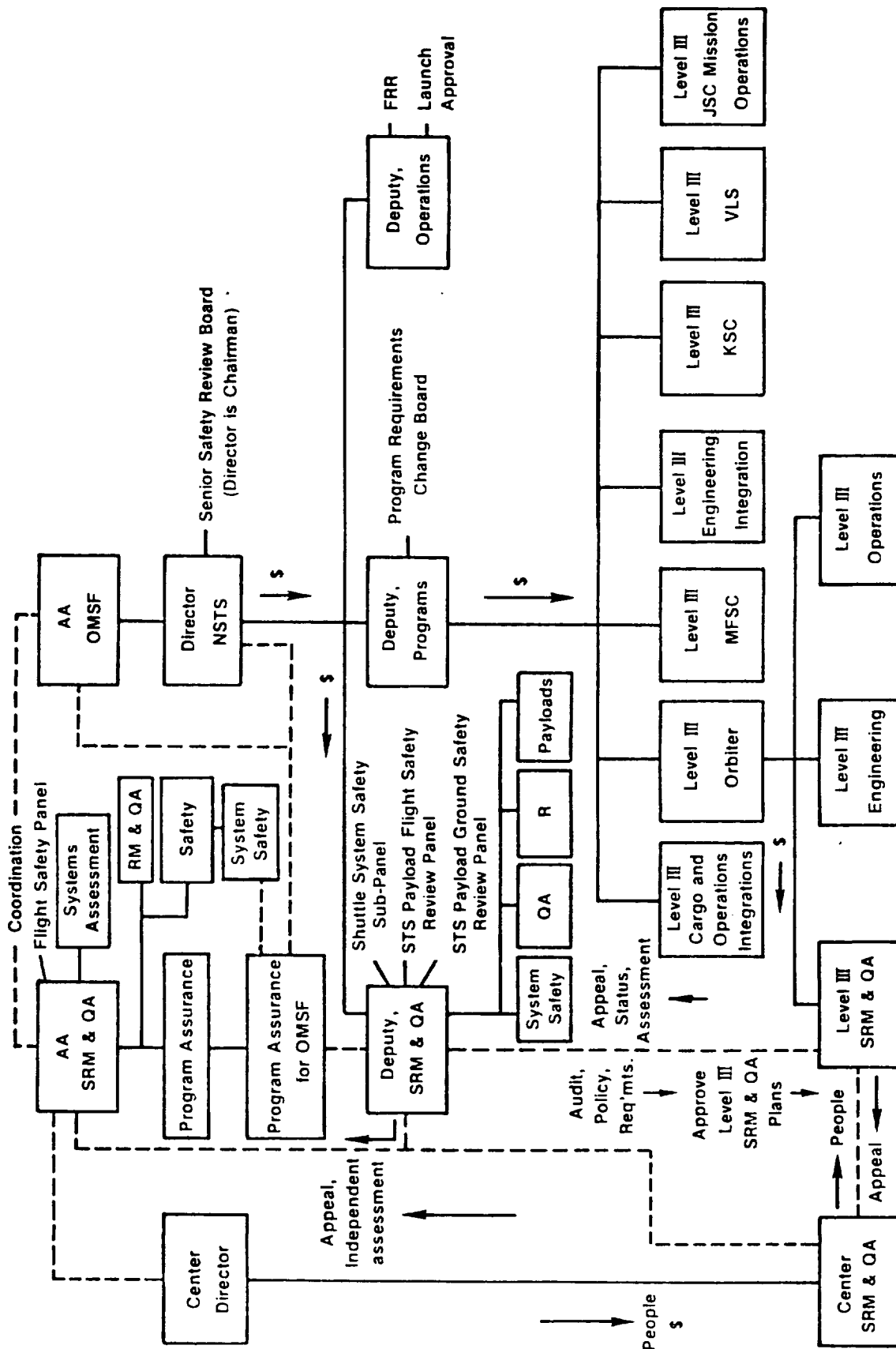


Figure 1. The NASA/NSTS Safety Organization

There are many reasons that this should be done over and above the added responsibilities recommended by this Committee which are inherent in the direction of the safety review boards, and the increased integration responsibilities. It is a fact of life that the higher level of management will bring a stronger voice in assessing the trade-offs in design changes, the resolution of technical issues which might affect safety, and the essential apportioning of resources to get the job done.

Also elevating the position to Program Deputy Director status would give the assurance disciplines a seat in the vital quorum for program decision making along with operations and engineering. Elevation of SRM&QA to Program Deputy Director status would assure that safety issues are brought to the attention of top management at NASA along with operations and engineering issues. This is essential in making sure that safety features are economically built in rather than expensively added as an afterthought or as a result of an oversight or accident.

Another advantage of this plan is that it demonstrates top management's resolve to infuse a higher level of safety, quality and reliability into every process involved with manned space flight. It helps to dispel those internal and external criticisms of NASA that "nobody really cares about safety."

3. RECOMMENDATION:

- a. Revise both program and assurance organizations in accordance with Figure 1 to foster independent safety assessment. Prioritize filling those positions essential to the safety assessment process at all levels of management. The support contractor's organization should also reflect this same independence.
- b. Revise the roles and responsibilities of the assurance managers and engineers to reflect the new concepts involved in "independent safety assessment."
- c. Develop memoranda of understanding for those organizations involved in furnishing matrixed support and for each individual involved in a matrix job.
- d. Reorganize and redefine the roles of the safety assessment review groups at all levels to separate the responsibilities of program and assurance management.
- e. Develop and publish a matrix of responsibilities for assurance functions in order to assure that each organization involved knows its role in both the primary risk assessment process and the independent review process.
- f. Develop a plan for implementation of independent safety assessment which addresses the short-term and long-term objectives, activities, and inputs necessary to make the launch decision.

C. THE CODE Q SYSTEM SAFETY ORGANIZATION

1. OBSERVATION:

Organizational roles, responsibilities and activities within Code Q fragment the system safety efforts and preclude a Level I independent risk assessment.

2. DISCUSSION:

The present Code Q organization splits the responsibilities for system safety among the System Safety Branch, the Operations Safety Branch

and Program Assurance Division. This in effect makes the Director of the Safety Division the day-by-day functional head of system safety and forces a complex and extensive coordination role between these three organizational elements. There are very few management systems that cannot be made to work. However, the dominant question in this case is "how efficient and how thorough can the job be done?"

There is little doubt that the system safety function is complex. It starts with design concepts in making sure that basic safety requirements are built into hardware and software designs for ground support equipment, facilities and flight systems. Also the function should be deeply involved in the identification of hazards and defining requirements in the fabrication time period. It is essential that continuity of this effort be maintained through the verification and prelaunch ground test periods. If risk is to be minimized, each step of the operation up to launch, flight and post flight must be analyzed for hazards and controlled.

All of this activity builds from the concept to completion of mission with a meticulous corporate memory of hazard controls, design, performance and safety margins, and verification and validation testing. System safety should be an integral part of this activity as a generator of basic safety requirements, a monitor to assure that the requirements are met and that the risks are clearly identified and dispositioned.

To manage all of this efficiently, Code Q needs a single manager for system safety not only to minimize redundancy but to simplify coordination of the system safety efforts throughout NASA and the contractor organizations.

Another problem with the Code Q organization exists in the present concept of approving hazard dispositions, Failure Modes and Effect Analyses and Critical Item Lists at or prior to Level II approval. This makes the Code Q organization a part of the program management in-line function and precludes it from being a part of the Level I independent safety assessment.

3. RECOMMENDATION:

- a. Consolidate the Code Q system safety function under one manager and change the roles and

NASA Headquarters Safety Division Organization

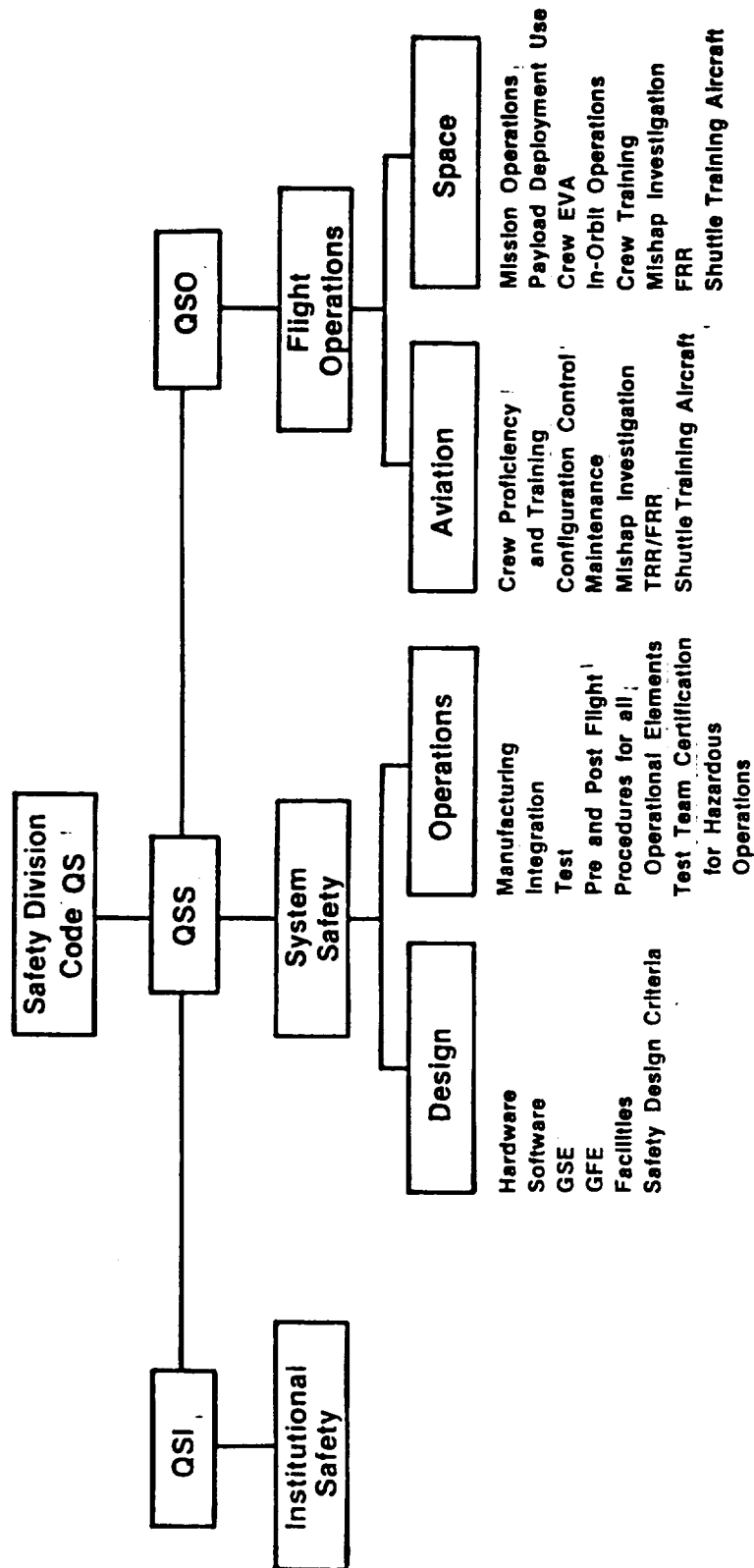


Figure 2 NASA Headquarters Safety Division Organization

responsibilities within Code QS to reflect the organization shown in Figure 2. The suggested functional statements of responsibility are discussed in Appendix D.

- b. Define interfaces, coordination requirements, and time related inputs between system safety and the other functions in Code Q responsible for the independent safety assessment.
- c. Remove all elements of Code Q from the in-line approval cycle for program reliability and safety analyses and documentation.

D. Management Within the NSTS Program

OBSERVATION:

There appears to be general confusion in the NSTS program as to what the total safety effort is or what it should be to effectively develop and manage aggregate safety risks.

DISCUSSION:

Most of the NSTS managers interviewed by the Committee knew very little of the mechanics or the principal instruments of risk assessment used in safety management. In addition, it was obvious that they did not have a clear picture of what the roles and responsibilities of each organizational element were or should be in accomplishing the total safety assurance effort.

While part of this confusion can be attributed to the vagaries of an unrecognized hybrid safety management (see Section V Background, page 17), there are other factors which appear to be contributing to this condition.

First there was a conscious reduction of NSTS management from rigorous safety oversight with the announcement that the NSTS was operational. The words used by some of those interviewed were "we had to become lean and mean." In fact the lean and mean translated to not much more than signature approval with no resources for any significant oversight. In turn, this philosophy led to an attrition of experienced people and fostered a communications and understanding gap between NSTS line and safety management.

At the same time there was a reduction of contractor management from the integration effort (both in-line and safety engineering), and there was a perceived handoff of integration responsibilities between contractors. It was obvious to the Committee that there were some safety responsibilities dropped and some others not clearly spelled out in this handoff. It also appears that this withdrawal resulted in the deterioration of communications between element contractors.

One suggested method for improving this situation is the adoption of a crew chief concept for shepherding critical flight systems from the manufacturing process through all of the operations leading to launch.

Another factor contributing to the lack of understanding of safety appears to be a general feeling that the safety inputs to the program have not been significant in the past. As a result there is a general attitude summed up by one comment, "Why should I learn what they (safety) do and how they do it when I can't use it."

Still another factor leading to confusion on NSTS safety issues and objectives is the "shoot the messenger syndrome". There were many comments on the hesitance of individuals to be the bearers of bad news. There were some examples of people who had been such messengers and who had incurred a gamut of criticism ranging from displeasure to outright wrath.

Also, there is evidence that even the astronauts may be reluctant to complain because of the fear of being prevented from flying. All of this has led to poor communications and a situation where problems, if surfaced at all, may not be dealt with in the proper manner.

In order to improve those communications vital to safety throughout the NSTS program, all managers of the program and every element of the program, including contractors, should be bound by a written management policy directing the exposure of potential safety concerns. Beginning with top management, there should be a critical evaluation factor written in every manager's performance appraisal which requires that manager to actively support free and open communications in all areas of safety disclosure.

In summary, there are processes and operations in the NSTS program that are not being properly evaluated for safety risks, e.g. no integrated hazard assessment. The Committee found no evidence that this was

recognized or that it would be addressed in the safety reassessment efforts. Also there is a general lack of understanding of the hazard identification, control and dispositioning process by NSTS management and their contractors. This could be improved by training. Lastly, there is a vital need in the reassessment process to revise not only the roles and responsibilities of the NSTS line and safety managers but individual "mind-sets" to think in terms of thorough and independent safety assessment - a new concept for NASA.

3. RECOMMENDATION:

- a. Develop a NASA system safety training program specifically oriented to program and project managers.
- b. Make Code Q a part of the existing NASA management training programs, including the Middle Management Education Program, Senior Executives Education Program, Management and Supervisory Training, and other Career Development Programs in both formal and informal sessions.
- c. Develop a decision flow diagram to identify all essential steps and organizational responsibilities in the safety decision process. This would clarify the process and identify the information and appeal avenues to all those organizations having essential inputs to the process.
- d. Develop an integrated hazards assessment which includes the design, processing, handling, and shipping, and the operations performed by all NSTS/NASA and contractors' organizations.
- e. Redefine program integration management to include primary responsibilities for each part of the NSTS system from design through manufacture to complete assembly, operation, launch, landing and maintenance.
- f. Adopt the "crew chief" concept for flight critical systems.
- g. Immediately develop and implement an audit plan to periodically review the NASA organizations and contractors at all management levels of the NSTS program to assure that the system safety functions are being adequately managed. Conduct a safety

audit of the entire NSTS program prior to the next launch.

- h. NSTS management should issue a policy statement to the individuals on the NSTS program soliciting their input on safety problems and reemphasizing the necessity of their inputs to assure NSTS mission success.
- i. Develop and implement a management instruction requiring management support for disclosure of safety problems with no fear of reprisal.
- j. Include a critical evaluation factor in every NSTS manager's performance appraisal which requires his/her support for free and open disclosure of safety problems.

VI. POLICY AND REQUIREMENTS

The NASA and NSTS system safety policies and requirements were reviewed, and an attempt was made to develop the documentation tree beginning with Level I requirements which would establish the minimum system safety requirements for the NSTS program.

1. OBSERVATION:

There is a lack of consistency in the interpretation and implementation of NASA and NSTS system safety policies and procedures among the NASA centers and among contractors.

2. DISCUSSION:

There are major gaps in tracing the NASA system safety policies and requirements from a Level I NASA document down through the NSTS program. The NASA policy which would direct the applicability of system safety to the various NASA systems has never existed. A NASA management issuance would be necessary to establish these requirements. The specific requirements for "manned rated" also needs to be addressed for spaceflight, Space Station, and other programs where man's presence in space is essential.

A System Safety Handbook which provides guidelines has been in existence since 1970. A revision of this document was in the final coordination cycle at the time of the 51L accident, however the publication of this document has been delayed to incorporate some additional changes to strengthen the system safety program even more.

The lack of an overall agency policy for system safety has resulted in confusion whenever program requirements need to be specified. Countless hours have been spent deliberating on whether the requirements imposed for a NSTS element in NHB 5300.4(1D-2) or the requirements imposed for an NSTS payload in NHB 1700.7A or both are applicable to programs like Centaur, Spacelab, Space Telescope, Space Station and many others. Depending on the choice made, there can be major differences with regard to the scope and depth of the analyses, safety reviews, and assessments. These differences hinder a consistent review and evaluation process applicable to NSTS elements, cargo, and payloads. The differences in these two NASA documents and the DOD implementing directives are illustrated in Appendix E, Table I.

In addition, none of the NASA Handbooks specifies the various hazards analyses, and some of the contractors do not know the proper hazard analysis methodology to use. It is important from an overall program point of view to be able to compare hazards from the various program elements and to know that the particular hazard level in each is essentially described the same way. It is also important to know the thinking process that was used in the development of a particular hazard report to be able to assess the completeness and accuracy of the analysis effort reported to NASA. Finally, it should be a requirement for the development of a meaningful data base if there is to be consistency in the way hazards are assessed and risks accepted.

Top level NSTS safety program requirements are published in NHB 5300.4(1D-2), however it is limited in its applicability as an integration requirements document. The document uses the word "provisions" in its title and refers to requirements only when speaking of contractors; "guidelines" is used when referring to the NASA centers. Program requirements should be specified and levied on all NASA management levels and contractors to assure consistency in implementation.

Within NHB 5300.4(1D-2), there are also conflicting definitions for safety categorization. The document contains safety definitions for catastrophic and critical hazards which are related to the time available to control the hazard and reliability definitions for criticality 1 and 2 part failure which relate to severity. This is confused even further if NHB 1700.7A is also applicable to the program because the severity definitions in that document are not consistent with those in NHB 5300.4(1D-2). Severity should be described by one set of definitions for management review and approval of the disposition of hazards and the acceptance of safety risks. Also the definition of "failure" does not address anomalies of design expectations. Cracked turbine blades of the Shuttle main engines are not viewed as a failure even though the engineers performing the design did not expect the blades to crack and many of the flight crew do not believe analysis is a justification for flying with potentially cracked blades. The cracked blade problem is discussed in some detail to provide an example of the implications of existing policy and definitions in providing a documented assessment of the safety risks for the NSTS.

While some of the arguments against accepting the risks involved in flying with cracked blades appear to

be emotional, there are many disturbing questions still unanswered in categorizing the problem such as:

- . How can it be said with any confidence that the blade cracks will never lead to catastrophic failure during the operation life cycle of the turbopumps if the failure mechanism is not known?
- . Are there stated values for the turbopump test and operations life cycle limits with clearly stated change-out requirements? If so, how were these limits determined?
- . Have the validation tests on crack propagation been conducted using actual flight stress profiles? If not, how have the uncertainties been resolved in calculating the life cycle risks?
- . Have all of the cracked blades had the same apparent failure and severity signatures?
- . What are the relationships between test and operations power profiles and cracked blades? If this has not been determined, are there any tests scheduled to determine this?
- . What, if any, is the relationship between tolerance buildup performance variations and the expected turbine blade operational stress profiles?
- . What are the tolerances in turbine blade materials strength and process controls? How do they relate to performance margins?
- . How accurate are the NDE tests in detecting material flaws? What are the acceptable flaw criteria? How have they been determined?
- . What has been done to date in fracture analyses? Are there any conclusions which have merit in providing a plausible explanation of the cracking phenomena?
- . Are there any relationships between blade cracking and the loads profile changes due to abnormal bearing temperatures and bearing wear?

The questions appear to be endless and many of them have undoubtedly been answered to some degree in the engineering management review process. As yet, there does not appear to be any effort to share this information in a review with the assurance community so that an independent assessment can be made of the

cracked blade risks. Changes in policy requirements and definition are required to emphasize the evaluation, abatement, documentation, and tracking activities for safety risks associated with these types of anomalies.

Also, within the NSTS program, there is very little control over the management level at which program requirements can be generated. Implementing documents for payload requirements in NHB 1700.7A can be found as center publications such as JSC 13830A rather than in Headquarters or NSTS Program documents. Auditing and traceability of compliance are complicated, fragmented and costly.

Answers to several questions indicated that some of the technical documentation in certain safety critical areas such as fracture control, pressure systems, ionizing radiation, etc., may be out of date or incomplete. If the design safety requirements do not reflect the latest technology and past lessons learned, the program can be in complete compliance with the specifications and standards and still present a situation where there are undisclosed inherent hazards in the design and operations.

Finally, there is presently no NSTS program document that defines the roles, responsibilities and authority of safety organizations and managers at each level in the program. Separate system safety plans exist for centers and contractors; however, an integrated system safety program plan which would describe interface and integration responsibilities does not exist. A safety management document is needed to describe the independent review and objective assessments that must be made at each subsequent level in going from Level IV to Level I.

3. RECOMMENDATIONS:

- a. Develop a documentation tree which would identify the baseline system safety program and design requirements that are applicable to all NASA programs including the NSTS program.
- b. Develop new documentation including an NMI for System Safety and requirements for manned rating which would establish top level policy.
- c. Revise the NASA Headquarters policy and requirements documents including the NHBs 1700.1, 1700.7A, and 5300.4(1D-2), to standardize content including key definitions.

- d. Revise NHB 5300.4(1D-2) so that it is directive on the NSTS program including the NASA centers. Revise definitions where necessary to provide clarification and eliminate conflicting interpretation. It is recognized that "grandfathering" provisions may be necessary.
- e. Develop an Integrated System Safety Program Plan for the NSTS program which reflects the safety risk management system requirements. Impose the plan by direction of program management and contractual requirements on all elements of the program.
- f. Conduct a review of all NASA Design Standards to reassess the adequacy of the safety requirements and margins.
- g. Develop "how to" documents which would dictate the hazard analysis procedures and format for common cause analysis, fault tree analysis, software safety analysis, and other safety analyses that may be of benefit to NASA.
- h. Establish a requirement for an independent safety review process for on-going high risk problems such as the SSME turbopump cracked blades to evaluate the level of risk and the risk assessment management criteria.

VII. SKILLED SAFETY PERSONNEL

As a result of Committee visits throughout the NSTS Centers, it became obvious that there was a shortage of skilled safety personnel throughout the entire NASA aerospace community.

1. OBSERVATION:

There is a critical lack of space systems engineering skills in NASA and its support contractors' safety organizations.

2. DISCUSSION:

In order to provide meaningful hazard analyses and safety assessments, safety engineers need to be competent not only in the system safety discipline but also in the areas of design, fabricating processes, test and all of the operational aspects of the hardware and software systems which must be evaluated for safety risks. If they do not, the hazard analyses, which are the cornerstones of the risk assessment, are usually incomplete and superficial. Also the analyses frequently lack all of the definitive safety margin specification procedures and validation requirements to assure adequate hazard controls. There is evidence that this is the case for many of the current NSTS analyses and the NSTS reassessment analyses.

If this situation is to be changed, the conditions which have caused the problem must be recognized and rectified. One of the principal reasons for the lack of space systems engineering skills in safety is the inability to convince the more promising engineers to choose system safety as a career field. Safety engineering has had an image of negativism. "This is the reason you shouldn't do this." The job has been viewed as a "look over the shoulder" rather than a doing function. As a result, those engineers who are identified as "on-the-fast track" prefer the design and operations disciplines. These disciplines provide more personal recognition and satisfaction and they usually lead to faster promotion. Also the journeyman positions for the line disciplines are a higher grade than those for the assurance disciplines.

It is unlikely that this situation will improve and unlikely that a meaningful safety assessment can be made without a change in management approaches and mind sets and a redirection of personnel resources. In the end, there must be recognition and rewards not only for the primary doer but also for those whose job

it is to question, probe and independently assess risk.

3. RECOMMENDATIONS:

- a. Develop and implement a structured career path for system safety engineering.
- b. Direct an immediate infusion of systems engineering people in the NASA safety and support contractors' organizations.
- c. Direct vigorous training programs in systems engineering for incumbent safety engineers.
- d. Upgrade the safety engineering and management positions to comparable status with line engineering.
- e. Rotate engineers from the line engineering and operation functions through the safety organizations. Assure that they will be given the option to return to their primary fields with the same upward mobility options as their peers who have not been assigned safety positions.
- f. Develop and implement NASA-wide, center managed, Safety Intern and Safety Co-op Programs.

VIII. PERSONNEL MOTIVATION

Throughout the interview process the Committee became aware of a lack of personal commitment to and identification with the NSTS program by the assigned personnel. It appears that many individuals working on the NSTS program have lost their motivation for excellence.

A. PROGRAM IDENTIFICATION AND MOTIVATION

1. OBSERVATION:

Personnel involved with the NSTS primarily identify with their own organization, element, project or function rather than with the program as a whole.

2. DISCUSSION:

A team spirit and pride of accomplishment must be rekindled. The importance of space venture must be reemphasized and the importance of personal integrity must be made clear to every individual involved in the manned space program. The management has not addressed this issue and, although there are so many areas requiring their attention, this pride must become an everyday part of the program if excellence in workmanship is to return to the program. This attention to detail and excellence must come from the personal motivation of every individual in the program.

There must be a renewed emphasis on a coordinated personal and team motivation program. The program should be one which does something positive to keep high morale and keen interest in job excellence. It should also be a program which constantly reevaluates its effectiveness, concepts and objectives and uses innovative ideas and new initiatives while providing job recognition and satisfaction. No matter how good the program is at the start, if it is not progressive and dynamic, it will eventually become ordinary, routine, and boring, and will lose its effectiveness. If this happens, there will be an increased risk of failures and accidents caused by carelessness and apathy.

3. RECOMMENDATION:

- a. Provide an NSTS program badge identifying all civil servants and support contractors working on the NSTS team.

- b. Reestablish a vigorous extensive Manned Space Flight Motivation Program. Emphasize the importance of manned space flight to national prestige, to the progress of science and technology and to the aspirations of mankind. Place the management of the program under Code Q to re-emphasize that honorees have excelled in their contribution to NSTS safety.

B. WORKMANSHIP AND QUALITY INSPECTIONS

1. OBSERVATION:

There is evidence that careless mistakes are still being made in workmanship in NSTS processing and not all of the quality checks which are necessary to assure that each job is done properly are being made.

2. DISCUSSION:

Substandard workmanship is basically a management problem. It requires persistent NASA management oversight at all critical activities, constant vigilance in first-line supervision and personal integrity on the part of each worker. It requires personal motivation that goes beyond the pay check. Each worker has to know that his or her job is important and he/she must have pride in accomplishment.

Much of the inspiration for excellence in workmanship, personal integrity and the notion that we should look beyond our individual jobs in making sure that risks for space travel are minimized has been lost over the years. It is not too difficult to understand this in light of the perceived routine nature of space flight.

It took the rude shock of the Challenger disaster to bring us to the reality that manned space flight is not routine. It takes the same attention to detail and the same personal integrity and dedication to excellence in workmanship for each flight as there was for the first flight and during the days when the initial space quests inspired all of us.

3. RECOMMENDATIONS:

- a. Reinstate a strong NASA management oversight of daily operations including "walk-arounds" by managers at all levels.
- b. Conduct more frequent SR&QA audits of contractors to review quality of work and assure compliance with SR&QA contract requirements.
- c. Make sure that supplies and vendors of NSTS materials and parts understand the importance of their products to the manned space flight programs.

C. SAFETY MOTIVATION PROGRAM

1. OBSERVATION:

There appears to be frustration and a lack of motivation on the part of the safety personnel involved with the NSTS program.

2. DISCUSSION:

There has been a general upheaval within the NASA safety organization as a result of several changes in safety management at Headquarters and the Manned Space Flight centers. All of the safety organizations were in a state of transition with new SR&QA Directors at two centers announced the same week of the Committee visit. Anticipated changes in personnel assignment and supervision, lack of well-defined objectives, and heavy workload were some of the factors causing a sense of frustration among safety people. This is naturally to be expected with all the changes being introduced. With time, some of this confusion will undoubtedly disappear as new people settle into their jobs.

This frustration coupled with the lack of career opportunities and their experience in an apparent "no win" situation have left the safety people very disgruntled. If the safety function is to become effective, the individuals that perform the safety function must be provided with the stimulus to be actively involved and utilized in the NSTS program. The stimulus must come from management and should be along the lines of improved respect and importance of each safety individual.

It is expected that positive effects will result if career development and training plans are implemented and individuals see a means to achieve their career objectives. Another aspect of motivation is recognizing each individual as a member and important contributor of a team which is working toward making the NASA Safety Program the best in the nation.

A motivational program should be established to include an inter-center safety working group of the Manned Space Flight Centers and contractors. Semi-annual meetings should be held to identify and discuss interorganizational problem areas, share innovative system safety techniques and exchange engineering and safety information essential to the NSTS program. This will provide a forum for information exchange that is separate from the decision-making activities of the safety review panels. Consideration should be given to inviting the major payload contractors.

To effect greater awareness of the NASA Safety Program and its people, it is suggested that an Annual NASA/Industry Safety conference be held. Another motivational tool which worked well in the past was the publication of a Headquarters SR&QA newsletter to assist in information distribution and team building.

3. RECOMMENDATION:

- a. Develop and implement a strong motivational program for the safety people involved with the NSTS program.
- b. Develop and implement a strong motivational program for safety personnel agency-wide to achieve improvement for all NASA programs.

IX. SAFETY ASSESSMENT REVIEW PROCESS

During visits to the three NSTS centers and Headquarters, the Committee reviewed the process by which hazards are identified and assimilated by safety management and by which safety risks are assessed and accepted by program managers.

1. OBSERVATION:

The present safety assessment review process is obscure.

2. DISCUSSION:

Most NASA and contractor organizations were in the process of reinstituting the safety assessment review process that existed for the early NSTS flights. Most organizations were preparing for the reviews that would be needed as part of the hazard analysis rebaselining effort. Much of the discussion centered around the contents and mechanism for updating the Mission Safety Assessment Report (MSAR).

The MSAR is a listing of hazards, hazard controls, and referenced the Critical Items List, but it does not provide an overall program assessment of the risk burden that the NSTS Program Manager would assume. The MSAR was reduced after the STS-4 flight to consideration of the differences between flights. The MSAR was generated by the safety organizations and was unknown to some managers and not understood by others. A conclusion that might be drawn from this is that the MSAR was not used by NASA management in engineering or launch management decisions. Also, the safety managers, not the program managers, were accepting the safety risks.

There appears to be some confusion as to the safety goals of program management because of the lack of program direction to centers and contractors. When individual managers were questioned about criteria used in accepting risks, none of those interviewed had any written criteria. Most of the managers could not explain how they would decide to accept or reject a particular risk. Some managers had not thought about why they accepted a particular risk in the past. Some stated, "Engineering (or safety) recommended it. That's good enough". Many managers assumed that a written procedure would need to be followed to the letter and be too restrictive and inflexible. On the other hand, the problem in having no criteria could result in acceptance of a risk at too low a management

level and a loss of awareness of a critical risk by upper management.

It was the opinion of many of the organizations visited that the safety reviews conducted by the Shuttle System Safety Panel and the Senior Safety Review Board were not in the mainstream of NSTS program decision making and therefore not effective in providing NSTS managers with the safety impact of the decisions made by them. Even the safety review process for payloads, while it is recognized as one of the better safety reviews conducted within the NSTS program, was questioned about the rigor of the review and the need for a more formalized process to address hazards and validate hazards controls in manufacturing, ground handling and operations. It was also recognized that this was probably due to the lack of personnel resources to allow sufficient pre-review preparation by the NSTS Payload Safety Review Panels.

This preparation for the NSTS payload safety reviews should include an extensive plan and structuring of the formal review process and should establish a minimum technical quorum for the formal meetings.

Finally, from the standpoint of the overall program, the safety assessment process has not changed since the 51L accident, and there is apparently no planning underway to change it.

3. RECOMMENDATION:

- a. Define the safety assessment process from Level I through Level IV including risk assessment criteria in a program level risk assessment and management document. Such a document should be promulgated by the NSTS Program Director to specify to all subordinate organizations how the program will identify, access and accept safety risks.
- b. Modify existing charters and reconstitute the membership of the safety assessment review groups to strengthen the technical capabilities and improve their effectiveness in the mainstream decision making.
- c. Provide personnel resources for the NSTS Payload Flight Safety Review Panel to allow more extensive planning and structuring of the formal review process.
- d. Revitalize the Mission Safety Assessment Report process to reflect aggregate risk including

special emphasis on modifications, trends,
identification of critical margins, and mission
pertinent operational and maintenance analyses.

X. REASSESSMENT OF STS HAZARD ANALYSES

Most of the organizations visited by the Committee had hazard reassessment efforts in progress. The efforts varied from a cursory review of existing hazard analyses to comprehensive reassessments including some additional independent analyses.

A. COMMON CAUSE ANALYSIS

1. OBSERVATION:

There are no plans for reevaluating the validity of the redundancy rating on the Critical Items Lists against common cause failures which might cause loss of redundancy and eventual loss of vehicle.

2. DISCUSSION:

There are some failure modes in systems which can result in loss of redundancy in a component or system with a single possible event, by coupling effects in an adjacent system, or with an environmental or operational condition or a generic fault. In order to properly evaluate these conditions, the safety engineer usually conducts a "common cause" hazard analysis. If done properly, such an analysis, as a minimum, would be used to:

- a. Identify those hazardous conditions leading to the loss of redundancy.
- b. Evaluate the engineering design, test and performance data which supports the safety margins and validation of redundancy.
- c. Make recommendations for alternate designs or design features to reduce risks of loss of redundancy where possible.
- d. Stipulate the specifications for control of the common cause failures. If this is not possible due to the maturity of the design or lack of data, there should be recommendations for testing and analysis leading to the definition of these specifications.

While the "O" ring design for the SRM which led to the Challenger accident was eventually recognized as not being truly redundant due to a generic fault, it would have been recognized prior to the

first launch if a proper common cause hazard analysis had been conducted.

This observation begs the question "what other items in the 1R and 2R criticality categories are there which should be given a different level of scrutiny and control and recategorized if necessary?" Or put another way "Are there any other hidden single point failures that are masked by the redundancy label?"

Present NSTS safety policy does not require that common cause hazard analyses be done, and there are no plans to do such analyses as a part of the safety reassessment program.

3. RECOMMENDATIONS:

- a. Immediately change the NSTS safety policy to require common cause hazard analyses for all criticality 1R and 2R items.
- b. Conduct common cause analyses on all criticality 1R and 2R items prior to the next launch.
- c. Provide a uniform method to conduct hazard and failure analyses including policy, ground rules, guidelines and definitions necessary to make the analyses thorough, consistent in content and responsive to the needs for safety evaluation during all phases of development and for independent safety assessment during the operation phase.

B. HAZARD CONTROLS

1. OBSERVATION:

There is no system to verify that each hazard control stipulated in the hazard closure review process is actually being implemented.

2. DISCUSSION:

Many NSTS program engineers and managers interviewed by the Committee were of the opinion that once a hazard was closed it was not a matter for concern. In addition, there seemed to be very little appreciation that the hazard reduction embodied in the controls does not change the hazard severity but rather reduces the probability for an accident. As a result, there is very

little follow-up to assure that the hazard controls are actually in place.

A part of this problem stems from the hazard closure criteria in NHB 5300.4(1D-2) which places emphasis on "residual" hazards and from an eagerness to reduce the number of items for management concern. There appears to be a lack of understanding of the fact that a "controlled" hazard which inadvertently does not have stipulated controls in place is just as dangerous as an "accepted risk" hazard which has no effective controls.

3. RECOMMENDATION:

- a. Change the definition and the discussion on page 2-5 of NHB 5300.4(1D-2) to emphasize that only if a hazard is totally eliminated through design can it be forgotten. All hazard have some residual risk, whether or not the hazards are controlled.
- b. Develop a management system to track and verify hazard controls.

C. MISSION OPERATIONS

1. OBSERVATION:

The NSTS mission operations functions are dispositioning risks which are not a part of an independent safety assessment process.

2. DISCUSSION:

The flight operations functions have traditionally been thorough in preparation for mission control. Likely flight anomalies and worst case mission scenarios are developed and simulations conducted to assure that the mission control teams can expeditiously handle flight emergencies. Cargo interfaces, both hardware and software, and likely flight anomalies are tested against realistic mockups of the shuttle vehicle. The real-time and near real-time technical assessment back-up for missions is continually tested and verified. Flight teams are trained in meticulous detail for their roles in the mission. All of this appears to be done with a high level of personal motivation and competence.

In all of this process there are inherent risks which are being identified, evaluated and dispositioned. As an example, the back-up mission control at GSFC is not manned in real-time. Presumably if it were necessary to use this capability, key people would have to be dispatched from Houston to man the facility. This appears to be a conscious decision that has been reached after evaluating the potential for complete loss of control at Houston due to likely facility failures or catastrophic events and the resulting effects on some interruption of real-time mission control.

There are similar risks which are being dispositioned in every decision being made in the development of the all important mission rules. While in retrospect, considering the excellent record of these operation functions, it appears that very little improvement could be made in the manner in which the tasks are being performed, there is the question of independent assessment. At present, many of the flight operation risks are not reflected in the overall mission safety assessment documentation and do not pass through the safety review process.

3. RECOMMENDATION:

- a. Develop policy and requirements to provide risk management inputs to the independent safety assessment organizations from the flight operations functions.
- b. Review the flight operations functions to determine if there are management and personal motivational techniques which could profitably be used by other NASA organizations.

XI. LAUNCH DECISION WAIVER PROCESS

The Committee reviewed the process of evaluating launch readiness and the decision making process in accepting or rejecting waivers to the launch decision.

1. OBSERVATION:

The criteria and ground rules leading to acceptance of waivers in the launch decision process are not clearly defined.

2. DISCUSSION:

Waivers are a part of life in the launch process. If it were a requirement to have a perfect space vehicle and perfectly functioning ground support equipment in order to launch, there would be no launches.

At the same time there have to be some hard and fast rules for evaluating the merit of waiver requests in order to reduce the risks and subjectivity of the decision process.

In the past emotion has played an inordinate part in the decision process. A former NASA program manager testifying before Congress in their investigation of the Challenger accident stated that people who have a pending problem "should come forward with a loud voice . . . They should have been kicking and screaming. You have to deal with hand wringing. I have never been where people aren't wringing their hands worrying that things might be bad."

Some of the managers who are in key positions in the launch decision process loop have expressed a viewpoint that there will always be some subjectivity and emotion involved in balancing safety, cost and schedules. One of these managers described the situation by saying, "In the end, someone has to suck up his gut and give the order to launch or scrub. In reaching this decision, the decision maker must be wary of both the hand wringers and the sunshine people who gloss over any problem that might delay launch."

While it is doubtful that the waiver and launch decision processes will ever be or should be completely unemotional, it is dangerous to depend on emotion as a major discriminator for risk. To assure that those processes are orderly, complete and devoid of emotion to the maximum extent possible, there should be ground rules and requirements for presenting waivers. Also, a clear definition of roles and

responsibilities is needed to assure that the proper people are evaluating the merits of the requests and are involved in the decision process.

3. RECOMMENDATION:

- a. Redefine the roles and responsibilities of organizations and people in the waiver and launch decision processes.
- b. Develop the criteria and ground rules for processing waivers and making launch decisions including guidelines for resolution of issues and avenues of appeal for higher level management decision.
- c. Establish minimum standards and requirements for presentation and consideration of waivers including information and data defining:
 - (1) Magnitude of deviation from stated launch and flight rules,
 - (2) Possible impact and consequences of waiver,
 - (3) Impact on hazard analysis or criticality classification in Critical Items Lists in any area of the NSTS program,
 - (4) Any prior risk assessments which might impact overall assessment including similar systems and operations,
 - (5) Statements of critical assumptions made in modeling and other engineering analyses on hardware and software involved and description of the impact of uncertainties in using the model to evaluate the mission environment,
 - (6) Status of validation for safety margins including test and flight measurement data,
 - (7) Analyses of problems affecting safety experienced prior to waiver requests on subject systems,
 - (8) Critical history or pedigree of hardware/software involved, and
 - (9) Any perceived uncertainties or unknowns in any information presented.

XII. SAFETY REQUIREMENTS IN THE NSTS CONTRACTS

During the course of the Committees review, it became increasingly clear that NASA relied heavily on contractors for safety support with primarily award fee contracts. The Committee reviewed these contracts to determine how safety requirements were being managed and how the entire award fee process was being implemented.

A. SAFETY PLANS

1. OBSERVATIONS:

System safety plans are used primarily to fill an initial contract deliverable requirement and are not updated or used in the management of the contract.

2. DISCUSSION:

Most contracts required a system safety plan be submitted and approved by the contracting officer. In at least one case, this was the primary output of the system safety program because the contract had not specified that the plan be implemented.

The initial system safety plans were developed generally to satisfy a deliverable requirement and, for this purpose, thoroughly addressed the safety engineering and management activities and resources and staffing requirements. But as the NSTS program changed and moved into the operational phase and as the safety emphasis waned, the system safety plans were not updated, resubmitted for approval, or utilized in project management. A revised system safety plan would have reflected a change in the scope of activities and a reduction in personnel. Another indication that system safety plans are of little significance are that audits of contractors apparently did not address how well the contractor was complying with the NASA approved plan. If the audits had been properly conducted, the need for updating the plan would have been evident.

A document that is important enough to be a deliverable and that reflects the agreement between NASA and the contractor on how the safety requirements are to be managed should be configuration controlled. This lack of emphasis in properly specifying system safety contract requirements can, to some degree, be attributed to

changes and the resulting deletion of system safety requirements in the procurement regulations.

The Committee could find no evidence that any of the system safety plans were used by NASA during the management of the contract. The plans contained no specific safety information on which the contractor could be evaluated for award fee purposes.

The overall system safety plan should be the basis for a System Safety Management Plan. In turn this plan would define the exact safety related activities that would be evaluated during each six-month evaluation period. This in conjunction with specific task assignments issued for system safety related work would provide a baseline for the evaluation. The System Safety Management Plan approach should also be used in evaluating Safety Services level-of-effort and "task assignment" contracts, where an overall system safety plan was not required to be submitted.

3. RECOMMENDATION:

- a. Reinstitute a NASA procurement regulation for specifying system safety requirements and contract deliverables that should be considered in procuring flight hardware and software, support equipment, facilities and services.
- b. Develop a System Safety Management Plan for all NSTS award fee contracts to evaluate the safety related activities.
- c. Place System Safety Plans under configuration control to assure changes are made when necessary.

B. AWARD FEE FOR SAFETY

1. OBSERVATION:

In most NASA contracts there were no special provisions for safety to be weighted and scored separately for the award fee. In those contracts where safety was considered a separate evaluation factor, there appeared to be a lack of consistency among the way evaluations are made and, in the end, too consistently high a grade being given for safety.

2. DISCUSSION:

Although some award fee evaluators thought they were evaluating safety and all of the fee was considering safety, this may not be the case. By not specifically telling the contractor the areas of concentration for award fee evaluation, the contractor cannot tell in which area the Government expects them to place management emphasis. If safety is important, then the contractor must see this in the written plan against which their performances will be evaluated. The attitude that, "if they mess up on safety then we will hit them hard," is after-the-fact management and goes against the intent of the award fee approach.

In some cases, there was confusion on how to develop, implement, and manage the award fee contract so that the contractor would be motivated to place special emphasis on safety. None of the NASA managers interviewed had been trained in the award fee process, and several managers expressed the need for formal training based on difficulties they were experiencing in the management of their contracts.

A review of the fees earned revealed that most of the award fee grades were in the ninety percentile range. The approaches being applied did not appear to be rewarding the contractor for better than normal performance nor was it penalizing them for less than satisfactory performance in safety or any other area. If the contractor starts out with a grade of satisfactory and then is graded up or down depending on the strengths or weaknesses, the contractor will be awarded a fee more representative of his performance. It appears the NSTS award fee approach is to start the contractor at a grade of 100 and grade down based on weaknesses. NASA also appears to have been placed in a defensive posture by having to explain to a contractor how he can earn 100 percent of the award fee. Also, the contractor is being paid a large fee to manage their performance. NASA should not direct contractor management actions and then be expected to objectively evaluate them.

An agency policy on award fee contracts should be developed and particular attention given to the grading system and the categories of grades, their definitions, the percentage of fee for each category and the grade to start from in applying strengths and weaknesses.

3. RECOMMENDATION:

- a. Dedicate a meaningful amount of award fee for safety with evaluation criteria based on a written system safety management plan for each evaluation period.
- b. Conduct a full review of the NSTS contracts using a team of NASA award fee experts not involved in the NSTS program to determine the effectiveness of the way safety requirements are being implemented and managed.
- c. Develop an agency policy on the implementation of award fee contracts with special emphasis on safety where appropriate.
- d. Implement a formal training course on award fee type contracts and make attendance mandatory for those individuals involved in the NSTS program award fee process.

XIII. SAFETY ASSESSMENT INFORMATION SYSTEMS

Every organization visited by the Committee expressed an interest and a need for utilizing existing data outside their organization. Database systems are being developed by different organizations without consideration of the NSTS as a total program.

1. OBSERVATION:

Details for safety assessment information data systems are being developed without comprehensive identification of need and front end planning.

2. DISCUSSION:

An accurate and timely information system should be the "life blood" of any independent safety assessment for launch. The first step in structuring such a system is to define exactly how the assessment job will be done. It is counterproductive and wasteful to develop information systems prior to taking this first step. After this is done, basic questions that need to be answered are:

- . What specific information is needed?
When is it needed and where?
- . What portion of the data needed exists?
Where?
- . What part of the total needs can be generated
within existing systems?
- . How can the voids in information needs be filled
after using existing systems?

It does not appear that this basic planning and job definition have been completed; nevertheless there has been considerable effort expended in Code Q to develop a detailed data system.

On the other hand, one center's safety organization is looking into the possibility of structuring its safety assessment information system around some 26 operational and engineering data systems already in place. In turn all of the contractors and many of the NASA organizations have internal data banks that are used for risk definition and assessment which are accessible by fundamental PC technology. There is a considerable effort and expense in maintaining these systems. There is also a great amount of information in these systems which can be used in common by many of the organizations involved in NSTS program.

Each of the organizations visited by the safety assessment committee were queried as to its need for data to do safety management. The majority agreed that their systems were adequate for most of their own needs, but they discerned a possible savings and more accuracy and efficiency in doing their jobs, especially in interface safety management, if they could have access to external data banks. It was also a general conclusion that such an interchange of safety information could accelerate the implementation of mishap fixes and lessons learned fixes to prevent similar mishaps.

Since many of the data banks are PC compatible, the technical problems in doing this appear to be minimal. In some instances there are some obvious problems in protecting proprietary information, but these do not appear to be insurmountable with today's computer capabilities to lock-out and protect data. The major obstacle appears to be one of impetus in identifying all of the data sources and data file contents and negotiating for its use.

In addition to the obvious cost savings, "piggy backing" on existing data systems has another advantage. The information is most accurate and timely at the place it is being generated. Each time it is removed and structured for another purpose, it presents a risk of being lost and possibly misunderstood. For these reasons a concerted effort should be made to limit the unique Code Q safety structured systems to a minimum. Conversely a maximum effort should be expended in determining what can be done with existing systems to discern safety critical trends and margins and answering such questions as:

- . How should the data be coded and filtered to assure rapid access, proper level of analysis, and protection from information glut?
- . How should data be retrieved and displayed?
- . How can the data system be maintained and updated to protect against errors, unauthorized use and data loss?

3. RECOMMENDATION:

- a. Identify the basic needs for data and information to make independent safety assessments.
- b. Make a survey of contractor and NASA organizations to determine the availability of information required to make the independent safety

assessment. Where necessary, negotiate for possible additions to these information systems.

- c. Develop a plan for the independent safety assessment information system to use the available data base systems and to structure those "delta" systems necessary to augment them. This should include a milestone schedule for implementation and should address interim options to provide the necessary information for independent safety assessment prior to completion of the fully developed system.
- d. Develop a safety information system to permit interactive access by NASA and contractor safety organizations to existing and new data files.

XIV. LIST OF RECOMMENDATIONS AND ACTION RESPONSIBILITIES

A summary list of the recommendations and organizations responsible for lead actions are as follows:

	<u>RECOMMENDATIONS</u>	<u>ACTION RESPONSIBILITY</u>
IV.A.3.a.	Immediately provide adequate resources for safety management and maintain a consistent level of effort through periods of success as well as periods of adversity.	HQS/A
	(1) Obtain a firm management commitment required to implement the Conceptual Plan for a NASA Headquarters Enhanced Safety Program.	HQS/QS
	(2) Update and distribute an approved implementation plan annually to include long range projected needs.	HQS/QS
	(3) Evaluate center level implementation plans and apprise NASA top management of major differences between the needs of the organization and actual resources.	HQS/QS
IV.B.3.a.	Develop a National Space Policy and NASA top level requirements for manned space flight and make the commitment to safety a part of this National Space Policy.	HQS/M
IV.B.3.b.	Demonstrate commitment and resolve for safety in the development of a NASA top level management policy.	HQS/Q
IV.B.3.c.	Assure that line managers down to first-line supervisors have a healthy concern for their role in providing safe flight.	HQS/M
IV.B.3.d.	Make the commitment to safety a stated and integral part of each manager's career development.	HQS/A
IV.B.3.e.	Evaluate the safety performance of each supervisor as part of their annual appraisal.	HQS/M

V.A.3.a.	Immediately take action to build a strong uniform system safety organization at Headquarters and throughout NASA.	HQS/Q
V.B.3.a.	Revise both program and assurance organizations to foster independent safety assessment. Prioritize filling those positions essential to the safety assessment process at all levels of management. The support contractor's organization should also reflect this same independence.	HQS/Q and HQS/M
V.B.3.b.	Revise the roles and responsibilities of the assurance managers and engineers to reflect the new concepts involved in "independent safety assessment."	HQS/Q
V.B.3.c.	Develop memoranda of understanding for those organizations involved in furnishing matrixed support and for each individual involved in a matrix job.	STS/I, II and III
V.B.3.d.	Reorganize and redefine the roles of the safety assessment review groups at all levels to separate the responsibilities of program and assurance management.	STS/I
V.B.3.e.	Develop and publish a matrix of responsibilities for assurance functions in order to assure that each organization involved knows its role in both the primary risk assessment process and the independent review process.	HQS/Q and HQS/M
V.B.3.f.	Develop a plan for implementation of independent safety assessment which addresses the short-term and long-term objectives, activities, and inputs necessary to make the launch decision.	HQS/Q
V.C.3.a.	Consolidate the Code Q system safety function under one manager and change the roles and responsibilities within QS to reflect the proposed organization.	HQS/QS
V.C.3.b.	Define interfaces, coordination requirements, and time related inputs between system safety and the other	HQS/Q

functions in Code Q responsible for the independent safety assessment.

- | | | |
|----------|---|-----------------|
| V.C.3.c. | Remove all elements of Code Q from the in-line approval cycle for program reliability and safety analyses and documentation. | HQS/Q |
| V.D.3.a. | Develop a NASA system safety training program specifically oriented to program and project managers. | HQS/QS |
| V.D.3.b. | Make Code Q a part of the existing NASA management training programs, including the Middle Management Education Program, Senior Executives Education Program, Management and Supervisory Training, and other Career Development Programs in both formal and informal sessions. | HQS/N |
| V.D.3.c. | Develop a decision flow diagram to identify all essential steps and organizational responsibilities in the safety decision process. This would clarify the process and identify the information and appeal avenues to all those organizations having essential inputs to the process. | STS/I |
| V.D.3.d. | Develop an integrated hazards assessment which includes the design, processing, handling, and shipping, and the operations performed by all NSTS/ NASA and contractors' organizations. | STS/II |
| V.D.3.e. | Redefine program integration management to include primary responsibilities for each part of the NSTS system from design through manufacturer to complete assembly, operation, launch, landing and maintenance. | STS/I |
| V.D.3.f. | Adopt the "crew chief" concept for flight critical systems. | HQS/M |
| V.D.3.g. | Immediately develop and implement an audit plan to periodically review the NASA organizations and contractors at all management levels of the NSTS program to assure that the system safety functions are being adequately managed. Conduct a safety audit of the entire NSTS program prior to the next launch. | HQS/Q and STS/I |

V.D.3.h.	NSTS management should issue a policy statement to the individuals on the NSTS program soliciting their input on safety problems and reemphasizing the necessity of their inputs to assure NSTS mission success.	STS/I
V.D.3.i.	Develop and implement a management instruction requiring management support for disclosure of safety problems with no fear of reprisal.	HQS/Q
V.D.3.j.	Include a critical evaluation factor in every NSTS manager's performance appraisal which requires his/her support for free and open disclosure of safety problems.	HQS/M
VI.3.a.	Develop a documentation tree which would identify the baseline system safety program and design requirements that are applicable to all NASA programs including the NSTS program.	HQS/QS
VI.3.b.	Develop new documentation including an NMI for System Safety and requirements for manned rating which would establish top level policy.	HQS/QS
VI.3.c.	Revise the NASA Headquarters policy and requirements documents including the NHBs 1700.1, 1700.7A, and 5300.4(1D-2), to standardize content including key definitions.	HQS/Q
VI.3.d.	Revise NHB 5300.4(1D-2) so that it is a requirement on the NSTS program including the NASA centers and contractors. Revise definitions where necessary to provide clarification and eliminate conflicting interpretation.	HQS/Q
VI.3.e.	Develop an Integrated System Safety Program Plan for the NSTS Program which reflects the safety risk management system requirements. Impose the plan by direction of program management and contractual requirements on all elements of the program.	STS/I
VI.3.f.	Conduct a review of all NASA Design Standards to reassess the adequacy of the safety requirements and margins.	HQS/Q

VI.3.g.	Develop "how to" documents which would dictate the hazard analysis procedures and format for common cause analysis, fault tree analysis, software safety analysis, and other safety analyses that may be of benefit to NASA.	HQS/QS
VI.3.h.	Establish a requirement for an independent safety review process for on-going high risk problems such as the SSME turbopump cracked blades to evaluate the level of risk and the risk assessment management criteria.	HQS/Q
VII.3.a.	Develop and implement a structured career path for system safety engineering.	HQS/Q and HQS/N
VII.3.b.	Direct an immediate infusion of systems engineering people into the NASA safety and support contractors' organizations.	HQS/A
VII.3.c.	Direct vigorous training programs in systems engineering for incumbent safety engineers.	HQS/Q
VII.3.d.	Upgrade the safety engineering and management positions to comparable status with line engineering.	HQS/A
VII.3.e.	Rotate engineers from the line engineering and operation functions through the safety organizations. Assure that they will be given the option to return to their primary fields with the same upward mobility options as their peers who have not been assigned safety positions.	HQS/A
VII.3.f.	Develop and implement NASA-wide, center managed, Safety Intern and Safety Co-op Programs.	HQS/QS and HQS/N
VIII.A.3.a.	Provide an NSTS program badge identifying all civil servants and support contractors working on the NSTS team.	STS/I
VIII.A.3.b.	Reestablish a vigorous extensive Manned Space Flight Motivation Program. Emphasize the importance of manned space flight to national prestige, to the progress of science and technology and to the aspirations of mankind.	HQS/Q and HQS/M

- Place the management of the program under Code Q to re-emphasize that honorees have excelled in their contribution to NSTS safety.
- VIII.B.3.a. Reinstate a strong NASA management oversight of daily operations including "walk-arounds" by managers at all levels. STS/I
 - VIII.B.3.b. Conduct more frequent SR&QA audits of contractors to review quality of work and assure compliance with SR&QA contract requirements. HQS/Q and STS/I
 - VIII.B.3.c. Make sure that supplies and vendors of NSTS materials and parts understand the importance of their products to the manned space flight programs. STS/I
 - VIII.C.3.a. Develop and implement a strong motivational program for the safety people involved with the NSTS program. STS/I
 - VIII.C.3.b. Develop and implement a strong motivational program for safety personnel agency-wide to achieve improvement for all NASA programs. HQS/QS
 - IX.3.a. Define the safety assessment process from Level I through Level IV including risk assessment criteria in a program level risk assessment and management document. STS/I
 - IX.3.b. Modify existing charters and reconstitute the membership of the safety assessment review groups to strengthen the technical capabilities and improve their effectiveness in the mainstream decision making. STS/I
 - IX.3.c. Provide personnel resources for the NSTS Payload Flight Safety Review Panel to allow more extensive planning and structuring of the formal review process. STS/II
 - IX.3.d. Revitalize the Mission Safety Assessment Report process to reflect aggregate risk including special emphasis on modifications, trends, identification of critical margins, and

mission pertinent operational and maintenance analyses.

- | | | |
|----------|--|--------------------|
| X.A.3.a. | Immediately change the NSTS safety policy to require common cause hazard analyses for all criticality 1R and 2R items. | STS/I |
| X.A.3.b. | Conduct common cause analyses on all criticality 1R and 2R items prior to the next launch. | STS/I |
| X.A.3.c. | Provide a uniform method to conduct hazard and failure analyses including policy, ground rules, guidelines and definitions necessary to make the analyses thorough, consistent in content and responsive to the needs for safety evaluation during all phases of development and for independent safety assessment during the operation phase. | HQS/QS |
| X.B.3.a. | Change the definition and the discussion on page 2-5 of NHB 5300.4(1D-2) to emphasize that only if a hazard is totally eliminated through design can it be forgotten. | HQS/Q |
| X.B.3.b. | Develop a management system to track and verify hazard controls. | STS/II |
| X.C.3.a. | Develop policy and requirements to provide risk management inputs to the independent safety assessment organizations from the flight operations functions. | STS/I |
| X.C.3.b. | Review the flight operations functions to determine if there are management and personal motivational techniques which could profitably be used by other NASA organizations. | HQS/Q and
HQS/M |
| XI.3.a. | Redefine the roles and responsibilities of organizations and people in the waiver and launch decision processes. | HQS/M |
| XI.3.b. | Develop the criteria and ground rules for processing waivers and making launch decisions including guidelines for resolution of issues and avenues of appeal for higher level management decision. | HQS/M |

XI.3.c.	Establish minimum standards and requirements for presentation and consideration of waivers.	HQS/M
XII.A.3.a.	Reinstitute a NASA procurement regulation for specifying system safety requirements that should be considered in procuring flight hardware and software, support equipment, facilities and services.	HQS/H
XII.A.3.b.	Develop a System Safety Management Plan for all NSTS award fee contracts to evaluate the safety related activities.	STS/I
XII.A.3.c.	Place System Safety Plans under configuration control to assure changes are made when necessary.	STS/I
XII.B.3.a.	Dedicate a meaningful amount of award fee for safety with evaluation criteria based on a written system safety management plan for each evaluation period.	STS/I
XII.B.3.b.	Conduct a full review of the NSTS contracts using a team of NASA award fee experts not involved in the NSTS program to determine the effectiveness of the way safety requirements are being implemented and managed.	HQS/H
XII.B.3.c.	Develop an agency policy on the implementation of award fee contracts with special emphasis on safety.	HQS/H
XII.B.3.d.	Implement a formal training course on award fee type contracts and make attendance mandatory for those individuals involved in the NSTS program award fee process.	HQS/H and STS/I
XIII.3.a.	Identify the basic needs for data and information to make independent safety assessments.	HQS/Q
XIII.3.b.	Make a survey of contractor and NASA organizations to determine the availability of information required to make the independent safety assessment. Where necessary, negotiate for possible additions to these information systems.	HQS/Q

- XIII.3.c. Develop a plan for the independent safety assessment information system to use the available data base systems and to structure those "delta" systems necessary to augment them. HQS/Q
- XIII.3.d. Develop a safety information system to permit interactive access by NASA and contractor safety organizations to existing and new data files. HQS/Q

APPENDIX A

CHARTER OF THE COMMITTEE

The memo from Mr. George A Rodney, Associate Administrator for Safety, Reliability, Maintainability, and Quality Assurance which chartered the STS Safety Risk Assessment Ad Hoc Committee on November 6, 1986, is included for background information.



National Aeronautics and
Space Administration

Washington, D.C.
20546

NOV 6 1986

Reply to Attn of

QSS

TO: Distribution

FROM: Q/Associate Administrator for
Safety, Reliability and Quality Assurance

SUBJECT: STS Safety Risk Assessment Ad Hoc Committee

I have tasked Joyce McDevitt, the NASA Headquarters System Safety Manager, to conduct a review of the STS safety risk management system and I solicit your support and cooperation in making this a truly worthwhile effort. Her Committee will include Louis Polaski from Ames Research Center, Richard Bright from Langley Research Center, Jonathan Mullin from Western Space and Missile Center, and four consultants - Charles Childs, Charles Mertz, Dan Neagu, and James Wiggins. Bill McCarty, Johnson Space Center, will be an observer to the Committee.

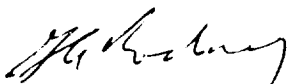
The Committee will conduct an independent and systematic assessment of the safety review requirements, process, documentation, and the safety organization's involvement in the STS Levels I, II, III, and IV decision process. The Committee is chartered to determine what the integrity of the entire NASA and NASA contractor safety risk management program was at the time of the Challenger mishap, what it is now, and what it will be in support of our next launch. The output will be a strengthening of our STS safety risk management program where necessary; a definition of the criteria, documentation requirements, and involvement of the Level I safety organization in the review and approval cycle; and an establishment of a safety risk management procedure that will be applied to all major NASA programs in implementing the enhanced NASA Safety Program. I have authorized the Committee to contact senior management, engineering, safety and, other personnel at whatever level they deem necessary.

The Committee will address the safety management system for all elements of the STS including flight hardware, payloads (NASA, DOD, and commercial), government-furnished equipment, ground support equipment, facilities, software, and normal and contingency operations. It will be especially helpful to the Committee if the organizations would also address those elements of the STS which present some uniqueness with respect to the safety requirements, management structure, and hazard analyses such as the Orbiter experiments, remote manipulator system, detailed science objectives, standard mixed cargo harness, standard switch panel, Spacelab, and STS/Space Station.

The schedule of activities in Enclosure 1 has been informally coordinated with your Safety Director and reflects a "bottoms-up" approach in reviewing Level IV organizations, first, wherever possible. It is requested that arrangements be finalized with each organization for the date shown with Johnson Space Center taking the lead to schedule Rockwell, Hughes, TRW, and Boeing; Kennedy Space Center to schedule Lockheed, McDonnell Douglas (Payload Operations Contract), Eastern Space and Missile Center, and Ebon; and Marshall Space Flight Center to schedule Rocketdyne, Morton Thiokol, USBI, McDonnell Douglas (Spacelab), and Martin Marietta. The Jet Propulsion Laboratory is requested to provide an insight into both the NASA and DOD payload safety review process. The Air Force Space Division/Western Space and Missile Center is requested to address both the payload and Vandenberg launch site activities. Each organization should assign a point of contact to work out the necessary details on time, location, briefing agenda, etc., with the Committee.

A list of questions is in Enclosure 2 to assist the organization in preparing for the briefing agenda. It is requested that the formal briefing be limited to one hour. To facilitate the review, the documentation and other information requested should be delivered to the Committee the day before the scheduled briefing. The advance information should also include a preliminary agenda with the names of the presenters.

It is essential that each organization share with the Committee an appraisal of both its strengths and weaknesses in the context presented so that NASA can have a safety risk assessment process that is independent, adequate, and timely. Your efforts in this regard are very much appreciated.



George A. Rodney

Enclosures

DISTRIBUTION:

JPL/L. Allen Jr.	AFSD/A. Casey
JSC/A. Cohen	
KSC/F. McCartney	
MSFC/J. Thompson	

cc:

M/R. Truly

ENCLOSURE 1

November	M	T	W	Th	F
17	Rocketdyne (SSME)	18 Rockwell Orbiter Int. Contr	19 WSMC (VLS & Payloads)	20 Hughes (Payloads)	21 TRW (Payloads)
24	JPL (Payloads)	25 Morton Thiokol (SRB)	26	27 THANKS- GIVING	28
8	At KSC Lockheed (SPOC)	9 At KSC McDonnell Douglas (POC)	10 At KSC USBI (SRB) ESMC (Payloads)	11 At KSC Safety Services Contractor (EBON) KSC (Payloads)	12 At KSC KSC (STS Processing) Level III
5	At MSFC McDonnell Douglas (Spacelab) Martin Marietta(ET)	6 At MSFC MSFC (payloads) MSFC (STS) Program Level III	7 Working Session At MSFC <u>TRAVEL</u>	8 At JSC STS Level IV STS Level III	9 At JSC STS Level II Payloads
12	At JSC Payload Safety BD Shuttle System Safety Panel Senior Safety Review BD Flight Safety Panel	13 At JSC Range Safety Astronaut Safety STS/Space Station Safety Services Contractor (Boeing) Working Session	14	15	16

AGENDA TOPICS (A) AND DOCUMENTATION (C)* TO SUPPORT THE
STS SAFETY RISK ASSESSMENT AD HOC COMMITTEE REVIEW

System Safety Requirements

(A) Describe the requirements which implement the safety review process in NHB 5300.4(1D-2) and NHB 1700.7A to include appropriate sections from the following:

- (C) Program/Project Directives
- (C) Specifications
- (C) Safety Plan
- (C) Internal Operating Instructions
- (C) Contractual Requirements Imposed On and by Your Organization
- (C) Other Program Plans Which Include Safety Requirements and Review Tasks
- (C) Other Documentation Which Describe the Safety Requirements Applicable to Planning, Design, Manufacturing, Testing and Operations

(A) Explain the contractor and subcontractor safety program.

(A) Describe your contract as to requirements, contract type, and the management interaction process between you and NASA.

(C) Provide a summary of the last three years available award versus earned fee.

(A) Describe the participation of safety personnel in the RFP preparation, contract evaluation, and contract negotiation.

(A) What are the lines of communication between the government and the contractor?

(A) What are considered to be the deliverables (plans, hazard analyses, hazard reports, safety assessment documentation), to the government? What is the procedure for obtaining government approval of the products?

Hazard Analyses

(A) How does the schedule for the hazard analyses effort provide for timely input into the design and operational activity?

(A) Describe the hazard analysis approach that had been used to assess the adequacy of the design, describe any differences in depth and scope of analysis at the system, subsystem, or component level, and the rationale used in tailoring the effort.

*Nine Copies Are Requested

(A) Describe the hazard analysis revalidation approach that is now being applied to assess the adequacy of the design and any new hazard analysis which will be performed. Describe the rationale for excluding certain areas.

(A) Describe the components, subsystems, or systems for which there will be an end-to-end (incoming inspection through fabrication, prelaunch checkout, launch, etc.) operational hazard analysis performed. Describe the rationale for items and areas excluded.

(C) Describe the techniques, formats, and instructions being used to perform the hazard analysis.

(C) Describe the procedures, technique, format, and instructions being used to conduct the safety evaluation of FMEA/CIL'S.

(C) Provide documentation that is typical of hazard analysis work sheets, hazard analysis results, and the closed-loop tracking system.

(A) Identify the initiator, reviewers, and approval authority for the hazard analysis reports and in tracking each hazard to verification of implementation. Provide forms which show individual signature authority if appropriate.

(A) Describe the change procedures used to ensure that hazards are updated as necessary to reflect proposed changes in the software and hardware configuration, procedures, environment, or management system.

(A) How are hazards which are disclosed by testing failures, nonconformances, mishaps, and in-flight anomalies incorporated into the hazard analyses?

(A) What mechanism is used to incorporate the operational data into updates of the hazard analyses?

(A) How are the results of hazard analyses communicated to the workers? What mechanism is used to solicit safety problems and concerns from the workers?

(A) What is the safety awareness training program for workers fabricating, assembling, handling, and transporting flight hardware?

Safety Risk Assessment

(A) Describe the hazard classification and risk acceptance criteria that are used to report and accept hazards. Describe

the responsibility and authority of the various levels of management (safety, project, etc.) in reporting, reviewing, and accepting safety risks.

(C) Provide a copy of the safety risk assessment report that is used to assimilate the safety data in a form useful to the decision makers.

(C) Provide copies of the initial and recurring safety risk assessment report.

(A) Describe the procedure used to assure a deliberate management decision to accept safety risks (singularly and cumulative).

Safety/Program/Design Reviews

(A) Describe the process by which safety requirements, hazard analysis results, safety risk assessments, and safety program concerns are addressed at the following as a minimum:

- Budget/Contract/Program Development Reviews
- Award Fee Board/Process
- System Requirements Reviews
- Preliminary Design Reviews
- Critical Design Reviews
- Design Certification Reviews
- Operational Readiness Reviews
- Test Readiness Reviews
- Flight Readiness Reviews
- Other Project Reviews (e.g., Packaging, Pre-ship)

(A) Describe the safety organization involvement in the above and the extent to which this involvement is independent and visible to the other elements of the organization.

(A) Describe the safety organization involvement in real time decisions that take place on a day-to-day basis subsequent to flight readiness review and to include the operation or launch commit decision.

(A) Describe the safety organization involvement in real time decisions that take place during the operation or flight to assure a successful mission. How does the responsible safety individual analyze flight data for safety implications?

(A) Describe the safety organization involvement in the post test, operation, or launch evaluation.

Closed-loop Procedures

(A) Describe the tracking system to assure that actions prescribed for hazard elimination or reduction are, in fact, implemented. Provide examples.

(A) Describe the tracking system to assure that hazards disclosed by test results, nonconformances, failures, anomalies, and mishaps are included in hazards analysis updates, addressed in the safety risk acceptance decision making process, and properly closed out. Provide examples.

(A) Describe the tracking system to assure that safety concerns raised at major reviews are properly addressed.

Audits

(A) Discuss the self (internal) audit program and its effectiveness.

(A) Discuss the effectiveness of the audit program implemented at the next organizational tier down or conducted from the next tier up.

Organization

(C) Organization chart developed in sufficient detail to understand the level (directoriate, division, branch, section, etc.) and line/staff functional responsibilities of each individual involved in the safety risk management process within the context of the entire organization and program.

(A) Describe the level of authority for the safety manager in the context of the total organization and program.

(C) Describe the total staffing, individual assignments, and internal structure of the organization element(s) responsible for STS safety.

(A) What are the qualifications and requirements (education, certification, registration, etc.) for the selection of safety personnel?

(A) What is the profile of the level of effort of the safety program over the duration of the STS program? Is the safety effort adequately funded?

(A) What is the level of effort for each activity of the safety program from establishing design criteria through recovery operations and post flight evaluations?

(A) Describe the involvement of all other organization elements which play a role in the safety risk management process.

(A) How do the individual safety personnel interface with people in other organizational elements (e.g., project, engineering, test, and operations)?

(C) Describe the charter and makeup of all boards, panels, and committees involved in the safety risk management process as to chairman, mandatory and associate membership, supporting personnel, and their location in the overall organization, frequency of meetings, input data and source, output data, and disposition.

(C) Provide a decision tree which describes the safety organization involvement and interface with all other appropriate organization elements to address the following as a minimum:

- Procurement Process
- Planning the Safety Program
- Performing Tradeoff Studies
- Identifying Hazards
- Documenting the Hazard Analysis
- Documenting the Safety Risk Assessment
- Accepting Safety Risks
- Implementing a Closed-loop Tracking System for Hazards
- Providing Safety Risk Visibility at Major Reviews
- Closing Out Safety Actions from Major Reviews
- Maintaining a Documentation Trail for Safety Concerns
- Receiving Safety Input from Organizations at a Lower Tier
- Providing Safety Output to Organizations at a Higher Tier
- Maintaining Currency on Configuration and Actions Taken
- Processing Engineering Change Proposals
- FMEA (CIL) Activity
- Failure Analyses and Quality Nonconformances
- Processing Deviations/Waivers

The flow diagram should address the entire decision process required to evaluate a change (design, material, procedure, etc.) from initiation of the change to acceptance and the safety personnel involvement in the change process.

(A) Discuss the safety management buy-off at decision points relating to:

- Design Verification Analyses and Testing
- Verification of Performance Margins
- Qualification and Acceptance Testing
- Hardware/Materials Delivery and Acceptance
- Transportation/Handling at and Between Launch Process Facilities

- Subsystem/System Assembly
- Assembly/Test/Checkouts at the Pad
- Prelaunch Review
- Countdown
- Launch Decision
- In-flight Controls
- Post Flight Analyses
- Recertification

(A) How does safety go about acquiring technical assistance if they need it?

(A) As a result of the Challenger mishap, have you changed your organization, what are the changes made, and the rationale if no changes have been made?

(C) Describe the organization elements and functional responsibilities related to:

- Quality
- Quality Engineering
- Quality Control
- Reliability
- Reliability Engineering

The relation of these functions and products to Safety, System Safety, System Safety Engineering, and Operational Safety Engineering.

Inhibitors/Barriers

(A) Describe any problems your organization has in fully implementing the NASA system safety policies.

(A) Describe any problems the safety organization has in providing an independent assessment of safety risks.

(A) Describe any problems the safety organization has with respect to its effectiveness and visibility in the decision making process.

(A) Describe any problems that exist with respect to the lack of, unclear or conflicting requirements.

(A) Describe any other problem you feel is appropriate to this review.

Recommendations for Improvement

(C) Provide any recommendations that should be considered in enforcing existing requirements, revising existing requirements, or developing new requirements to make the NASA and NASA

contractor safety programs aggressive, proactive, independent, and visible.

(C) Describe any recommendations that should be addressed in improving the safety risk management system in the external organizations with which you are required to interface, i.e., both at the tier below you and above you.

(C) Describe any system safety practices used by any other organization, e.g., DOD, DOE, ESA, or contractors, which you feel NASA could benefit from.

(C) Provide any other recommendations you feel are appropriate to this review

APPENDIX B

THE NASA/NSTS SAFETY ORGANIZATION

A restructuring of the NASA/NSTS organization along the lines of Figure B-1 is offered for consideration. The proposed organization separates the program SR&QA function from the center's assurance functions and, most importantly, adds emphasis to the program Level II SR&QA function. To provide further definition to the proposed organization, the roles and responsibilities associated with the major safety elements would include the following important features:

- a. Headquarters - One person from the Program Assurance Division would be assigned to be the single focal point for providing overview and coordination of SR&QA activities in the Office of Manned Space Flight Programs to the Associate Administrator for Safety, Reliability, Maintainability and Quality Assurance. Additional support, such as a Program Assurance Manager for the NSTS program and Expendable Launch Vehicles, may be required.

The Program Assurance Manager should be responsible for providing and coordinating NASA SR&QA policies and procedures with the NSTS Deputy Director for SR&QA and through the audit process assure program compliance with these NASA requirements. This manager would also provide the Associate Administrator for SRM&QA with a status on the NSTS program SR&QA activities. This position would be supported by other Headquarters Code Q personnel which should be organized along functional lines.

- b. NSTS Program Director - The NSTS Program Director should have the final decision authority in accepting safety risks. To concentrate on the safety issues prior to each flight, the NSTS Program Director would be appointed Chairperson of the Senior Safety Review Board.
- c. NSTS Deputy Director for SR&QA - This position should be established to provide the same position of authority for SR&QA as presently exists for Programs and Operations. The Deputy Director should be supported by a System Safety Manager who would be responsible for providing independent reviews of hazard analyses, FMEAs and CILS and would also be responsible for assuring that all safety issues across interfaces are identified and assessed. The Deputy Director for SR&QA would also be responsible for defining the charter, membership, and operating procedures for the Shuttle System Safety Panel, the NSTS Payload Flight Safety Review Panel and the NSTS Payload Ground Safety Review Panel. In addition, the Deputy Director should be responsible for performing

[illegible]

B-2

audits of the Level III SR&QA organizations and provide an appeal route for those organizations in resolving SR&QA issues. A significant feature of this position is the capability to draw on any NASA resources for safety, engineering, and operations expertise whenever it is needed, e.g. for a special ad hoc safety review. The Deputy Director would be responsible for developing the Mission Safety Assessment Report for the Flight Readiness Review.

- d. NSTS Level III SR&QA Organizations - These organizations should be manned by personnel matrixed from the center SR&QA organizations. These organizations would report directly to the Level III Program Office. The Level III SR&QA organizations should monitor and audit the Level IV SR&QA activities.
- e. Center SR&QA Organizations - These organization should provide the SR&QA personnel for the NSTS Level III SR&QA organizations. They would also have an audit function to perform of all programs at the center. An appeal route would exist to the AA/SRM&QA.
- f. Center Directors - They should provide the administrative support and personnel to support the NSTS program activities conducted at their respective Centers. They should support the AA/SRM&QA in developing the independent safety assessment and, in addition, provide an appeal route for critical safety decisions and problem resolutions.
- g. Senior Safety Review Board - The Chairperson would be the NSTS Program Director. The membership of the board would consist of the institutional Directors for Safety, Engineering and Operations through Level III to provide a final objective review of the safety issues considering their impact on design and operations. The Board would establish and apply criteria for the acceptance of risk for the NSTS program. If the "institutional" Safety Directors take exception to the final decision of the NSTS Program Director, an appeal route would exist to the AA/SRM&QA.
- h. Shuttle System Safety Panel - The Chairperson would be the System Safety Manager under the NSTS Deputy Director for SR&QA. The membership will include the Level III System Safety Managers with appropriate support from Level IV. The Panel would be established to provide the safety position for the Program Requirement Change Board (PRCB) review. The Panel would recommend criteria for acceptance of risks by the PRCB.
- i. Payload Safety Review Panels - The Chairperson and membership would remain unchanged but reporting would be to the NSTS Level II Deputy Director for SR&QA. This will strengthen the process of apprising NSTS program management on individual and cumulative safety risks.

APPENDIX C

THE SPACE STATION SAFETY ORGANIZATION

A proposed organization for Space Station is shown in Figure C-1 which parallels the suggested restructuring of the NASA/NSTS organization. The proposed Space Station organization separates the program SR&QA function from the center's assurance functions and introduces a Level A Prime Deputy Director for SRM&QA. This is provided as an example of an organizational approach that the Committee feels can be applied to provide both program SR&QA support and the independent assessment for other major NASA programs, including high risk flight test programs and the design of high risk experimental facilities.

The organizational chart for the Space Station Program is structured as follows:

- Center Director**
 - AA SRM & QA**
 - Systems Assessment**
 - RM & QA**
 - Safety**
 - System Safety**
 - Program Assurance**
 - Program Assurance for Space Station**
 - AA Office of Space Station**
 - Level A Prime Director Space Station**
 - Level A Prime Deputy Assistant Director**
 - Level A Prime Deputy SRM & QA**
 - System Safety**
 - QA**
 - R**
- Center SRM & QA**
 - Appeal, Status, Assessments**
 - Audit, Policy, Req'ts.**
 - Approve Level B SRM & QA Plans**
 - People**
 - Appeal**

Coordination (dashed line): Connects the Center Director to the AA Office of Space Station and the Center SRM & QA.

People (solid line): Connects the Center Director to the Center SRM & QA.

Level B Offices (connected to the Center SRM & QA):

- Level B MSFC Space Station Office**
 - Project**
 - Integration**
- Level B JSC Space Station Office**
 - Project**
 - Integration**
- Level B GSFC Space Station Office**
 - Project**
 - Integration**
- Level B LeRC Space Station Office**
 - Project**
 - Integration**

Other Offices (connected to the Level A Prime Deputy Assistant Director):

- Office of Administration**
 - Information Systems**
 - Program Control**
 - Operations**
- Office of Program Requirements and Assessment**
 - SE & I**
 - Utilization**
 - Int'l.**

C-2

APPENDIX D

THE CODE Q SYSTEM SAFETY ORGANIZATION

Consolidation of the Code Q system safety functions along the lines of Figure D-1 is offered for consideration. The proposed organization establishes a central authority for NASA-wide system safety policies and procedures, focal points for functional system safety disciplines, an organization that has no involvement in the day-to-day decision making on program system safety issues and therefore one that can provide a truly independent safety risk assessment of programs, and a cadre of system safety people for other Code Q program support/assessment activities.

It is proposed that the Safety Division be made of three branches as is now planned; the Institutional Safety Branch, the System Safety Branch and the Flight Operations Branch. Changes in functional statements of responsibility are proposed for the System Safety Branch and the Flight Safety Branch. No changes to the presently defined charter of the Institutional Safety Branch are proposed.

System Safety Branch - This Branch should be composed of two sections; Design and System Safety Operations. The Design section would be responsible for providing the NASA-wide system safety policies and procedures that are applied during the design phase of a program. Personnel in this section will normally attend program design reviews to obtain an overview of the design safety issues. They will perform audits of program and center system safety procedures related to design. The System Safety Operations section would be responsible for providing NASA-wide system safety policies and procedures that are to be applied during the manufacturing, integration, testing and operational phases of a program. Responsibilities for aircraft or space operations would be focused towards the hardware and software of the program and the ground support operations personnel.

The Flight Safety Branch should be subdivided into two sections; Aircraft Programs and Manned Spaceflight Programs. The Flight Safety Branch would be responsible for providing safety policies and procedures for the flight phases of these programs. Their responsibilities would be focused on the Flight Readiness Review process to assure that the flight hardware, software, procedures, flight crew and ground support personnel are ready to fly, and on the continuing operations activities.

NASA Headquarters Safety Division Organization

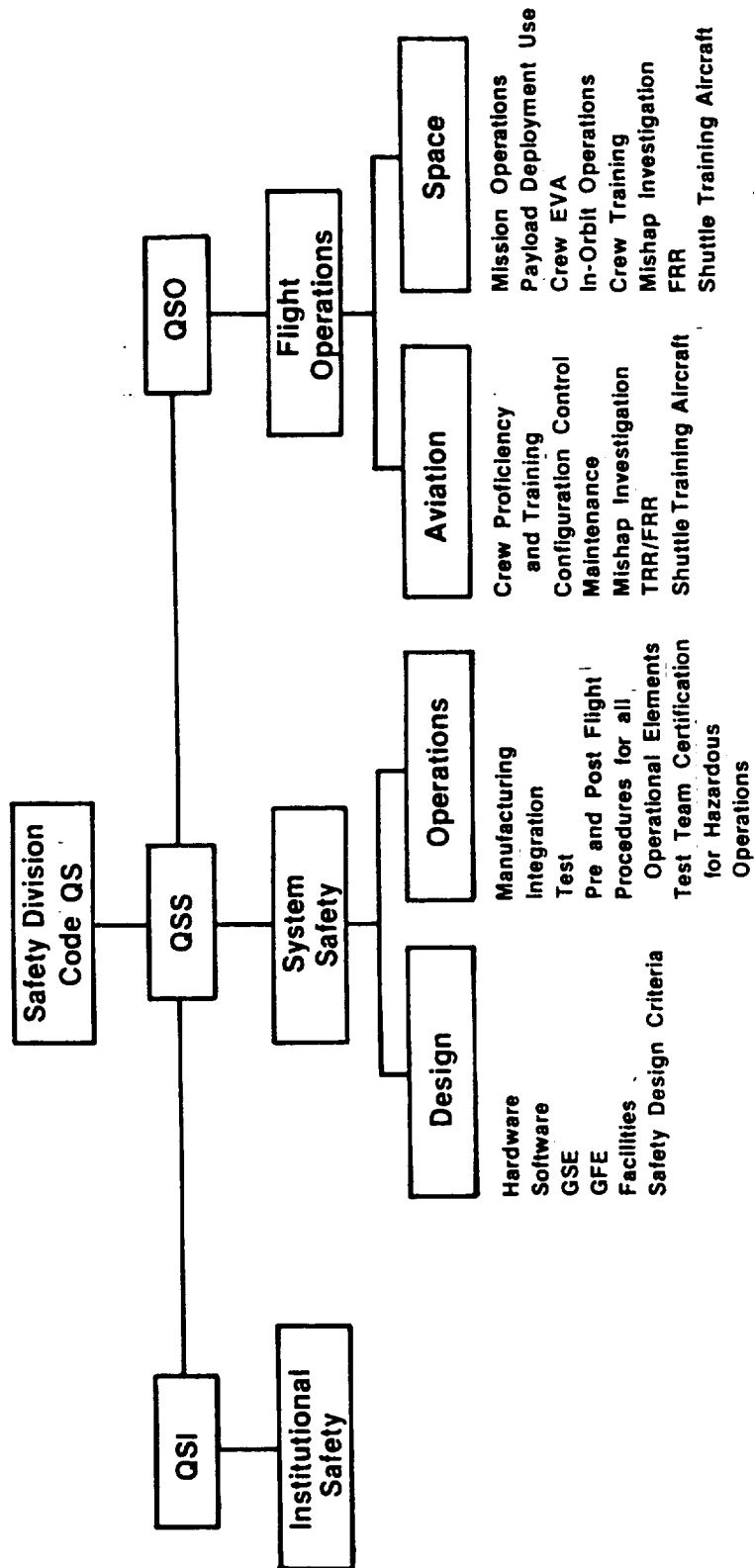


Figure D-1. The NASA Headquarters Safety Division Organization

APPENDIX E

NSTS POLICY AND REQUIREMENTS

This Appendix is a comparison of the requirements documents applied to the NSTS program. It illustrates the potential for confusion that exists on the program.

TABLE E-1 STS POLICY AND REQUIREMENTS DOCUMENTATION

TERMS	NHB 5300.4 (1D-2)	NHB 1700.7A	MIL-STD 1574 A
Catastrophic	An act or condition that results in a malfunction that causes a loss of personnel capability or loss of system with time to respond	Personnel injury Loss of Orbiter Loss of STS facility Loss of ground equipment	Use of MIL-STD-882B I. Catastrophic II. Critical III. Marginal IV. Negligible
Critical	An act or condition that results in a malfunction that causes a loss of personnel capability or loss of system with time to respond	Damage to STS equipment or requires use of contingency or emergency procedures	
Controlled	Application of HRPS	Not prescribed	
Residual Hazard	HRPS not developed or provided for a hazard	Not prescribed	Acceptable conditions specified
Fault Tolerance	CA Not prescribed CA Not prescribed	Two fault tolerance No single failure	Specified as acceptable conditions
Personnel Injury	Not prescribed except as related to catastrophic and critical definition	Loss of life, major injury, crew incapacity such as bone fracture, second and third degree burns, severe laceration, internal injury, severe radiation exposure, chemical or physical agent toxic exposure, unconsciousness	Major: Defined as admission to hospital bone fracture, second or third degree burns, severe lacerations, internal injury, severe radiation exposure, chemical or physical agent toxic exposure, unconsciousness
Safety Critical	System containing: hydraulic/pneumatic system, space hardware handling equipment electrical systems in a flammable environment, personnel working platforms, radiation, ordnance, pressure vessel, propulsion systems	Contains an element of risk	Any condition, event, oper. process, equipment, or system, with a potential for major injury or damage
Deviation	Granted use of an article which would not meet the specification before the fact	Not prescribed	An alternate method of compliance with the intent of specific req.
Waiver	Granted use of an article not meeting specification after the fact	Granted use of an article not meeting a specification	Not defined
Hazard Closure	1. HRPS - Design out 2. HRPS - Controls verified through test analysis training programme 3. Accepted by NASA	Not prescribed	Acceptable conditions specified
Quality Parts Concept	Quality of components a major concern	No concern for quality of components	Appropriate quality to meet acceptable conditions
Escape and Rescue	Abort	Not described	Not specified
System Safety Program Plan	Required	Not included	Detailed content
Qualified System Safety Engineer	Not included	Not included	Not included